PANORAMIC

GOVERNMENT INVESTIGATIONS 2026

Contributing Editor

Moritz Pellmann

Freshfields



LEXOLOGY

Government Investigations 2026

Contributing Editor

Moritz Pellmann

Freshfields

Panoramic guide (formerly Getting the Deal Through) enabling side-by-side comparison of local insights, including into enforcement agencies; forms of liability; requirements and trigger events for investigations; whistle-blower and employee protections; document preservation and production (including data protection, privacy, and legal privilege limitations); investor notification; cooperation with enforcement agencies; resolution of investigations; potential civil and criminal penalties; and recent trends.

Generated on: July 23, 2025

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2025 Law Business Research

Explore on **Lexology**

Singapore

Wilson Ang, **Jeremy Lua**, **Charis Low**, **Chen Yan Wang**, **Terence De Silva**
Norton Rose Fulbright

Summary

ENFORCEMENT AGENCIES AND CORPORATE LIABILITY

Government agencies
Scope of agency authority
Simultaneous investigations
Civil forums
Corporate criminal liability
Bringing charges

INITIATION OF AN INVESTIGATION

Investigation requirements
Triggering events
Whistle-blowers
Investigation publicity

EVIDENCE GATHERING AND INVESTIGATIVE TECHNIQUES

Covert phase
Investigation notification
Evidence and materials
Providing evidence
Employee testimony
Sharing information
Investor notification

COOPERATION

Notification before investigation
Voluntary disclosure programmes
Timing of cooperation
Cooperation requirements
Employee requirements
Why cooperate?
Privileged communications

RESOLUTION

Resolution mechanisms
Admission of wrongdoing
Civil penalties
Criminal penalties
Sentencing regime
Future participation

UPDATE AND TRENDS

Key developments of the past year

ENFORCEMENT AGENCIES AND CORPORATE LIABILITY

Government agencies

1 What government agencies are principally responsible for the enforcement of civil and criminal laws and regulations applicable to businesses?

Some of the key government agencies and their primary areas of enforcement are:

- the Commercial Affairs Department of the Singapore Police Force – serious fraud, money laundering and economic sanctions;
- the Monetary Authority of Singapore – securities and banking laws and economic sanctions;
- the Accounting and Corporate Regulatory Authority – accounting, financial reporting and business registration laws;
- the Competition and Consumer Commission of Singapore – competition and antitrust;
- the Corrupt Practices Investigation Bureau – bribery and corruption; and
- the Attorney-General's Chambers – the prosecution of offences.

Law stated - 2 July 2025

Scope of agency authority

2 What is the scope of each agency's enforcement authority? Can the agencies pursue actions against corporate employees as well as the company itself? Do they typically do this?

The Attorney-General's Chambers (AGC) is the principal prosecuting entity. The Attorney-General is the Public Prosecutor and has the control and direction of all criminal prosecutions and proceedings. The Crime Division of the AGC is responsible for all criminal prosecutions, including prosecuting offences and supervising prosecutions conducted by other government departments and agencies. The Crime Division comprises various specialised clusters, one of which focuses on prosecuting complex white-collar crimes, corruption and technology crimes.

The Commercial Affairs Department (CAD) of the Singapore Police Force is the principal white-collar crime investigation agency. It investigates complex fraud, financial crime and money laundering, which are criminalised through legislation such as the Penal Code 1871 (the Penal Code) and the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992. The CAD also investigates violations relating to United Nations (UN) sanctions implemented through the United Nations Act 2001, which applies to non-financial institutions and individuals.

The Monetary Authority of Singapore (MAS) regulates the financial industry and exercises its enforcement functions across the banking, insurance, capital markets and other related

sectors. It is responsible for enforcement actions arising from breaches of laws and regulations administered by MAS, which are set out in the Schedule to the Monetary Authority of Singapore Act 1970 (MAS Act), and includes legislation such as the Financial Services and Markets Act 2022 (FSM Act), the Securities and Futures Act 2001 (SFA), the Financial Advisers Act 2001 (FAA), the Banking Act 1970 and the Insurance Act 1966.

MAS is also responsible for issuing guidelines on money laundering and terrorist financing to financial institutions and conducting regulatory investigations on those matters, and it may refer potential criminal offences to CAD for further investigation. In addition, MAS investigates violations relating to UN sanctions implemented through regulations issued pursuant to the FSM Act, which apply to financial institutions.

The Accounting and Corporate Regulatory Authority (ACRA) regulates business registrations, financial reporting, public accountants and corporate service providers. It administers legislation such as the Accounting and Corporate Regulatory Authority Act 2004 and the Companies Act 1967. On 1 April 2023, the Singapore Accountancy Commission (SAC) and the Accounting Standards Council (ASC) merged as one entity, taking on the name of ACRA.

The Competition and Consumer Commission of Singapore (CCCS) is Singapore's competition regulator and consumer protection authority. It administers and enforces the Competition Act 2004, investigates anti-competitive conduct in Singapore and administers the Consumer Protection (Fair Trading) Act 2003.

The Corrupt Practices Investigation Bureau (CPIB) is responsible for investigating and preventing corruption, and is the only agency authorised to investigate corruption offences under the Prevention of Corruption Act 1960 (PCA). It may additionally investigate corruption-related offences in legislation such as the Penal Code.

The above agencies can pursue enforcement action against companies and their employees. The extent to which they pursue actions against both the company and its employees varies between agencies and is dependent on various factors, such as the specific legislation and nature of the matter being investigated. For example, where the contemplated enforcement action relates to a criminal offence that requires proof of a mental element (eg, corrupt intent or dishonesty), the agency may face evidential difficulties and decide to pursue action only against the employees; however, this is not necessarily the case, and there, nevertheless, may be sufficient means of proof or specific offence-creating sections for corporate criminal liability.

Law stated - 2 July 2025

Simultaneous investigations

3 Can multiple government entities simultaneously investigate the same target business? Must they coordinate their investigations? May they share information obtained from the target and on what terms?

Multiple government entities may simultaneously investigate the same business. They need not necessarily coordinate their investigations but may decide to do so.

Such coordination may be through formalised arrangements, ad hoc inter-agency taskforces or more informal means of cooperation. One example of a formalised arrangement is the CAD–MAS Joint Investigations Arrangement, under which the Commercial Affairs Department of the Singapore Police Force and Monetary Authority of Singapore collaborate to investigate all offences under the Securities and Futures Act 2001 and the Financial Advisers Act 2001.

Information obtained by government agencies through the exercise of statutory investigative powers may generally not be shared with other government agencies, except where the common law public interest exception or a specific statutory provision applies.

Law stated - 2 July 2025

Civil forums

4 In what forums can civil charges be brought? In what forums can criminal charges be brought?

Depending on the relevant legislation and the severity of the contravention, civil enforcement or regulatory actions can be brought by an enforcement agency either through the court system for civil claims or through out-of-court procedures arising from primary or subsidiary legislation. For instance, regarding contraventions of Part 12 of the Securities and Futures Act 2001 (relating to prohibited market conduct), the Monetary Authority of Singapore (MAS) may, with the consent of the Public Prosecutor, bring an action in court against the relevant person to seek an order for a civil penalty for that contravention.

MAS may also pursue other enforcement actions that are dealt with out of court, including withdrawal or suspension of licence or regulatory status, removal from office, prohibition orders, compositions, reprimands, warnings and letters of advice.

Criminal proceedings can only be brought in the courts.

Law stated - 2 July 2025

Corporate criminal liability

5 Is there a legal concept of corporate criminal liability? How does the government prove that a corporation is criminally liable for the acts of its officers, directors or employees?

Yes, there is a legal concept of corporate criminal liability. Various offences in criminal statutes (eg, the Penal Code 1871 and the Prevention of Corruption Act 1960) may be committed by a person. The term 'person' is defined in the Interpretation Act 1965 to include 'any company or association or body of persons, corporate or unincorporate' and has the aforementioned meaning unless 'there is something in the subject or context inconsistent with such construction' or the statute expressly provides otherwise. The Penal Code provides expressly that '[t]he word "person" includes any company or association or

body of persons, whether incorporated or not'. Most offences can, therefore, be committed by either a natural person or a corporation.

In *Public Prosecutor v China Railway Tunnel Group Co. Ltd (Singapore Branch)* [2025] SGHC 101 (*CRTG*), the High Court affirmed the current approach to attributing liability to companies for criminal offences such as bribery. To do so, the prosecution must show that the director or employee who committed the offence was either the 'living embodiment' of the company or had acted within the scope of a properly delegated management function (the *Tom-Reck* test). In *CRTG*, the Court found that the test was not met in view of, among other things, the corporate structure of the company (including the fact that the matter involved a branch of the company) and the specific factual circumstances that showed that the company did not condone the acts of the employees. There remains a wide range of circumstances where the *Tom-Reck* test would be fulfilled, and government investigations focused on corporate criminal liability are likely to persist.

For regulatory offences that impose obligations on the company itself, the High Court in *CRTG* recognised that it may be appropriate to formulate a special rule of attribution, having regard to the policy and purpose of the underlying legislation. Such a rule should be formulated with reference to employees responsible for fulfilling the relevant obligations, such as those involved in the company's operational or administrative functions. Attribution of liability to the company in such cases is more likely to arise where the company lacks adequate internal controls over the functions of those employees.

There may also be specific offence-creating sections prescribed for corporate criminal liability in legislation. For example, the prescribed test for attribution in relation to money laundering offences is found in section 73 of the Corruption, Drug trafficking and Other Serious Crimes (Confiscation of Benefits Act 1992 (CDSA), which provides that (1) where it is necessary to establish the state of mind of a company in respect of conduct engaged in by the company, it is sufficient to show that a director, employee or agent of the company, acting within the scope of his or her actual or apparent authority, had that state of mind; and (2) any conduct engaged in or on behalf of a company by a director, employee or agent of the company acting within the scope of his or her actual or apparent authority, or by any other person at the direction or with the consent or agreement (whether express or implied) of such director, employee or agent, shall be deemed, for the purposes of the CDSA, to have been engaged in by the company.

In relation to offences under Part 12 of the SFA (regarding prohibited market conduct), there are also statutorily specified situations (under sections 236B to 236D of the SFA) prescribing how the mental state and acts of managerial persons may be attributed to the company.

Law stated - 2 July 2025

Bringing charges

6 Must the government evaluate any particular factors in deciding whether to bring criminal charges against a corporation?

The Attorney-General's Chambers (AGC) has explained that key considerations in commencing prosecution include the sufficiency of evidence and the public interest in prosecuting the corporate offender. Other than that, there is no legal obligation for the government to evaluate any particular factor in deciding whether to bring criminal charges against a corporation. Ultimately, the decision whether to pursue a corporate entity for criminal conduct is a matter of prosecutorial discretion (see article 35(8) of the Constitution-).

In this regard, in November 2015, Singapore's then Attorney-General Mr VK Rajah SC authored an opinion in which he discussed Singapore's approach to corporate liability. Mr Rajah stated that 'both individuals and corporate entities can expect to face prompt enforcement action for financial misconduct', although '[t]he emphasis, if there is one, is placed on holding accountable the individuals who perpetuated the misconduct'; nevertheless, '[s]ignificant attention is also given to the culpability of corporations . . . especially if the offending conduct is institutionalised and developed into an established practice in an entity over time'.

Mr Rajah emphasised that 'the decision to take action against a corporate entity requires careful consideration in order to ensure that disproportionate collateral damage is not inflicted on innocent parties such as employees . . . as well as shareholders' and that a 'careful assessment of all competing interests has to be made when considering whether to prosecute a corporate entity'.

To date, the AGC has not made public any prosecutorial guidelines.

Law stated - 2 July 2025

INITIATION OF AN INVESTIGATION

Investigation requirements

7 What requirements must be met before a government entity can commence a civil or criminal investigation?

Investigations may generally be commenced when the government entity receives information about or is otherwise made aware of a potential criminal offence, regulatory breach or other potentially prohibited conduct. Some government agencies, such as the Monetary Authority of Singapore (MAS), are statutorily permitted under legislation such as the Securities and Futures Act 2001 to conduct investigations 'as it considers necessary or expedient' for various broad purposes.

Some agencies have provided guidance regarding when they will commence investigations. The Accounting and Corporate Regulatory Authority (ACRA), for example, has stated that it will consider three factors before deciding to conduct investigations: whether there is sufficient public interest to do so; the harm done by the alleged breach; and whether the complaint is bona fide and, if so, whether it contains sufficient information for ACRA to mount an investigation.

Law stated - 2 July 2025

Triggering events

8 What events commonly trigger a government investigation? Do different enforcement entities have different triggering events?

Common trigger events include reports filed with the enforcement agency (whether by a whistle-blower, a self-reporting company or otherwise), inter-agency referrals (including from foreign counterparts) and media coverage. Trigger events vary between different enforcement entities.

Law stated - 2 July 2025

Whistle-blowers

9 What protections are whistle-blowers entitled to?

There is presently no general or overarching legislative protection for whistle-blowers; however, there are some specific legal provisions setting out safeguards in certain situations.

Whistle-blowers are afforded some protection when they report potential contraventions of the Prevention of Corruption Act 1960 (PCA). Section 36 of the PCA safeguards the identity of whistle-blowers by providing that no complaints regarding an offence under the PCA shall be admitted in evidence in any legal proceedings, and no witness shall be obliged or permitted to disclose the name or address of any whistle-blower, or state any matter that might lead to their discovery. Further, the court may permit the concealment or obliteration of documentary evidence that could identify the whistle-blower to the extent necessary to protect the whistle-blower from discovery.

All companies listed with the Singapore Exchange (SGX) (ie, issuers) are required to put in place protections for whistle-blowers. Rules 1207(18A) and (18B) of the SGX Mainboard Listing Rules require all listed companies to put in place a whistle-blowing policy that sets out the procedures for a whistle-blower to make a report to the issuer on misconduct or wrongdoing relating to the issuer and its officers. The issuer must also explain in its annual reports how it ensures that the identity of whistle-blowers is kept confidential and its commitment to ensuring the protection of whistle-blowers against detrimental or unfair treatment, etc.

The SGX and Monetary Authority of Singapore (MAS) have further emphasised the need to protect whistle-blowers in the Code of Corporate Governance 2018 (last updated 11 January 2023) and the Practice Guidance of 14 December 2023, which recommend that the audit committee of the board of directors should have oversight over the significant matters raised through the whistle-blowing channel (and report to the board of directors on the same), and review the policy and arrangements for concerns about possible improprieties in financial reporting or other matters to be safely raised, independently investigated and appropriately followed up on.

Separately, an informant who reports information on cartel activity to the Competition and Consumer Commission of Singapore (CCCS) may be given an undertaking by the CCCS to keep the identity of the informant (and any information that may lead to their identification) confidential throughout the course of its investigation. The informant may also be granted immunity or leniency for cooperating with the CCCS by stepping forward with useful information on cartel activity they may be implicated in. In appropriate cases, a monetary reward can be paid to informants for information that leads to the CCCS securing an infringement decision against the cartel members.

Similarly, informants who report tax evasion or fraud to the Inland Revenue Authority of Singapore will have their identities and the information and/or documents provided by them kept confidential. The informants can request a reward based on 15 per cent of the tax recovered (capped at S$100,000), if the information and/or documents provided lead to a recovery of tax that would otherwise have been lost. The maximum reward of S$100,000 has been successfully claimed in the past.

Employment-based protections for whistle-blowers are set to expand with the Workplace Fairness Act 2024 (WFA), which was passed in January 2025 and is expected to come into force in 2026 or 2027. The Act prohibits retaliation against employees who report workplace discrimination or harassment and requires employers to implement fair grievance-handling procedures. 'Retaliation' is defined broadly to include dismissal, denial of re-employment, unauthorised salary deductions and other acts of victimisation. However, the WFA's scope is narrow: it applies only to internal reports of discrimination or harassment and does not extend to whistle-blowing on regulatory, financial or criminal misconduct.

Aside from the WFA, section 14 of the Employment Act 1968 protects employees who have been dismissed without just cause or excuse, by providing an avenue for seeking reinstatement or compensation against the employer. Employees who have been terminated as a result of their whistle-blowing can, therefore, seek such legal redress on this basis. Similar protection against retaliatory dismissals can be found in section 18(2) of the Workplace Safety and Health Act 2006.

Further, the Tripartite Guidelines on Fair Employment Practices issued by the Tripartite Alliance for Fair & Progressive Employment Practices (TAFEP) encourages employers to treat all employees based on merit at all phases of employment.

Whistle-blowers who feel victimised or discriminated against by their employers can seek help from the Ministry of Manpower (MOM) or TAFEP, who will then further investigate the allegations and consider enforcement action against the employer. This includes placing the employer on the Fair Consideration Framework watch list, asking the employer to rectify lapses in its human resource processes and, in more serious cases, curtailing the employer's ability to obtain approval from MOM for work pass privileges to employ foreign workers in Singapore.

Law stated - 2 July 2025

Investigation publicity

10 At what stage will a government entity typically publicly acknowledge an investigation? How may a business under investigation seek anonymity or otherwise protect its reputation?

The approach to the public acknowledgement of an investigation varies between government entities and also depends on factors such as the trigger event for the investigation. For example, where an investigation is conducted based on intelligence or a report lodged by a whistle-blower, the investigation may be made known only when action is formally taken against the company, such as when charges are brought in court or when penalties are imposed by the government entity.

Where there is existing press coverage, or there are reasons for publicity (eg, to ensure investor awareness), the government entity may disclose an investigation at the outset or while investigations are still ongoing. For example, MAS indicated in its Enforcement Report for July 2020 to December 2021 that it will provide 'updates on the status of selected major cases [which are still under investigation] . . . to provide greater transparency regarding [MAS's] efforts to pursue the cases'.

It is generally difficult for a company under investigation to seek anonymity, although the company may, in exceptional instances, be able to convince the government entity that premature disclosure of the company's identity would be prejudicial to, for example, the market value of its shares (if the company is a listed entity) or matters such as other ongoing litigation. The company may otherwise seek to protect its reputation through effective public relations management and ensuring cooperation with the investigating agency.

Law stated - 2 July 2025

EVIDENCE GATHERING AND INVESTIGATIVE TECHNIQUES

Covert phase

11 | Is there a covert phase of the investigation, before the target business is approached by the government? Approximately how long does that phase last?

An enforcement agency may conduct covert investigations prior to approaching the target business. This may be done where, for example, the agency has reason to believe that the target business may be highly uncooperative. A covert phase is not mandatory or necessarily standard practice, and there are no published guidelines or consistency regarding the length of such a phase. It depends on the circumstances.

Law stated - 2 July 2025

12 | What investigative techniques are used during the covert phase?

Common investigative techniques include obtaining information and documents from witnesses and other parties through interviews and production orders, accessing computers and entering premises without a warrant. Parties subject to such investigative techniques will be notified of the confidential nature of the investigations and that any steps taken to compromise the confidentiality of, and thereby interfering with, the investigation may constitute a criminal offence.

Law stated - 2 July 2025

Investigation notification

13 After a target business becomes aware of the government's investigation, what steps should it take to develop its own understanding of the facts?

Generally, after a target business becomes aware of a government investigation, it should retain external counsel to carefully scope, plan and execute an appropriate internal investigation to develop its own understanding of the facts; however, the target business should be careful not to take any steps that may constitute 'tipping-off', obstruction or interference with the government investigation.

Tipping-off is an offence under section 57(1) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA) and section 10B(1) of the Terrorism (Suppression of Financing) Act 2002. Interfering with a government investigation may also constitute an offence under section 204A of the Penal Code 1871 which, among other matters, criminalises the commission of an act 'that has a tendency to obstruct, prevent, pervert or defeat the course of justice', knowing that the act is likely to, or intending for the act to, obstruct, prevent, pervert or defeat the course of justice.

Consequently, when planning an internal investigation against the backdrop of an active government investigation, care should be taken to ensure that any investigative step undertaken will not have the effect of tipping-off or obstructing the course of justice. This may affect considerations surrounding the issuance of document preservation notices, corporate communications and interviewing employees and third parties.

The target business may also consider engaging with the appropriate law enforcement or regulatory agency conducting the investigation to coordinate or 'deconflict' potential investigative steps, such as conducting interviews or taking disciplinary measures.

Law stated - 2 July 2025

Evidence and materials

14 Must the target business preserve documents, recorded communications and any other materials in connection with a government investigation? At what stage of the investigation does that duty arise?

Generally, it is an offence under section 204A of the Penal Code 1871 for a person or entity to commit any act that has a tendency to obstruct, prevent, pervert or defeat the course of justice (with the requisite knowledge or intention for this to occur). This includes intentionally destroying documents or any other evidence that would likely be requested by the authorities in an investigation that has arisen.

Companies should be mindful not to commit the offence by, for example, taking steps to preserve the relevant evidence as soon as it is aware that an investigation has been commenced (ie, at the early stages of the investigation).

Law stated - 2 July 2025

Providing evidence

15 During the course of an investigation, what materials – for example, documents, records, recorded communications – can the government entity require the target business to provide? What limitations do data protection and privacy laws impose and how are those limitations addressed?

Enforcement agencies can generally require a target business to provide a wide range of materials. The nature and scope of the power to require the production of materials varies between government entities and depends on the entity's statutory powers. Pursuant to the Criminal Procedure Code 2010, for example, an officer of the Commercial Affairs Department of the Singapore Police Force or above the rank of sergeant has the power to require a person to produce 'any document or thing'.

The statutory powers of investigation of government entities are generally not limited by data protection and privacy laws. For instance, section 17(1) read with the First Schedule of the Personal Data Protection Act 2012 provides that personal data may be collected, used and disclosed by an organisation without the individual's consent if it is necessary for any investigation or proceedings in relation to the contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in the exercise of its powers under any written law.

Law stated - 2 July 2025

16 On what legal grounds can the target business oppose the government's demand for materials? Can corporate documents be privileged? Can advice from an in-house attorney be privileged?

First, the target business can seek to resist the government's order for the production of materials based on its scope. While the relevant statutory powers to request production of materials tend to be broad, the courts have upheld the principle that such powers to order production are specific in nature, and a general demand for unspecified documents would be inadequate; the documents required to be produced must be clearly specified, and the courts will not allow a demand that amounts to a 'fishing expedition'. It may, therefore, be possible to challenge an excessively broad and wide-ranging request on the ground that it extends to material that is irrelevant to the investigation.

In addition, the target businesses can seek to resist the government's demand for materials on the ground that such materials are protected by legal professional privilege. In this regard, apart from legal privilege arising from the engagement of external legal counsel, in-house counsel legal privilege is statutorily enshrined in sections 128A and 131(2)(b) of the Evidence Act 1893. Legal professional privilege also extends to in-house counsel providing legal advice in their capacity as the company's lawyer by virtue of the common law.

The extent to which a target business can resist the government's demand for materials on the ground of legal professional privilege depends on the nature of the investigation, the material under consideration and the relevant statute under which the investigation is commenced. The powers of investigation under certain statutes are expressly subject

to legal privilege (eg, production orders issued under section 36 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992), while other provisions (eg, sections 20 and 35 of the Criminal Procedure Code 2010 (CPC)) are silent regarding the interaction between legal privilege and the powers of investigation.

In *Ravi s/o Madasamy v Attorney-General* [2021] 4 SLR 956 (*M Ravi*), the Singapore High Court considered how a claim of legal privilege over documents lawfully seized by the Singapore Police Force under section 35 of the CPC ought to be handled. It stated, in obiter dicta, that seized materials subject to assertions of legal privilege are to be segregated and provided to a separate legal privilege team at the Attorney-General's Chambers (AGC), which is not involved in the prosecution or criminal matter and will review the privileged information and determine whether to accept or dispute the assertions of privilege.

If the AGC legal privilege team agrees that the material is legally privileged, the material will be set aside and returned to the party from whom it was seized. If the team disputes the assertions of privilege, the party who holds the privilege may either waive their claim to privilege (in which case the material will be provided to the investigating and prosecuting team) or maintain the claim by, for example, commencing judicial review proceedings against the AGC, where the assertion of privilege will be considered by the court.

While this decision is technically obiter dicta, it is significant for two reasons. First, it implies that the exercise of the powers of criminal investigation under the CPC may be subject to the operation of legal privilege, even though the CPC is silent on the application of legal privilege. Second, it establishes a clear procedure by which disputes over a party's assertion of privilege regarding material seized by a law enforcement agency exercising criminal powers of investigation under the CPC are to be managed.

Anecdotally, the procedure in *M Ravi* has been applied in Singapore where material asserted to be privileged is seized or ordered to be produced for the purpose of investigations. It nevertheless remains to be seen whether the applicability, scope and nature of the procedure will be clarified or refined by the High Court or the Court of Appeal in a subsequent judgment, having the benefit of full arguments on this issue, or by Parliament through enactment of legislation.

Law stated - 2 July 2025

Employee testimony

17 May the government compel testimony of employees of the target business? What rights against incrimination, if any, do employees have? If testimony cannot be compelled, what other means does the government typically use to obtain information from corporate employees?

Enforcement agencies have the power to interview and record statements from witnesses generally, including employees of the target business. As with other witnesses, the employee's right against self-incrimination is dependent on the nature of the agency's investigative power.

Where statements are recorded by the Commercial Affairs Department of the Singapore Police Force under section 22 of the Criminal Procedure Code 2010 (CPC), the witness

'is bound to state truly what [he or she] knows of the facts and circumstances of the case, except that [he or she] need not say anything that might expose [him or her] to a criminal charge, penalty or forfeiture'; however, where statements are recorded by the Corrupt Practices Investigation Bureau (CPIB) under section 27 of the Prevention of Corruption Act 1960 (PCA), there is no privilege against self-incrimination, and the witness is legally bound to 'give any information on any subject which it is the duty of the [CPIB officer] to inquire into under [the PCA] and which it is in [the witness'] power to give'.

While a witness may be under no legal compulsion to provide evidence, should they be later charged with an offence (and become an accused person), the court hearing the criminal proceedings may draw adverse inferences from their failure to mention any fact that they subsequently rely on in their defence – that fact being one that they could reasonably have been expected to mention upon being charged with the offence but on which they chose to remain silent (section 261 of the CPC).

Enforcement agencies may also obtain information from a company pursuant to general powers to order the production of documents or other materials, or to seize relevant materials through, for example, a dawn raid.

Law stated - 2 July 2025

18 Under what circumstances should employees obtain their own legal counsel? Under what circumstances can they be represented by counsel for the target business?

Generally, employees may cooperate with legal counsel of their company if their interests are aligned with the company and there is little risk of the employees themselves becoming the target of the government investigation. In those situations, the employees are essentially acting as representatives of the company.

Employees should obtain their own independent legal counsel if they are at risk of becoming the target of a government investigation themselves or if their interests are likely to diverge from that of the company. In this regard, it is not uncommon for companies to provide support for their employees who find themselves the target of government investigation alongside their employers, including the engagement of independent legal counsel to represent such employees.

Law stated - 2 July 2025

Sharing information

19 Where the government is investigating multiple target businesses, may the targets share information to assist in their defence? Can shared materials remain privileged? What are the potential negative consequences of sharing information?

Yes, targets in a government investigation may generally share information with each other to assist in their defence, provided that doing so does not cause the targets to fall afoul of tipping-off prohibitions or the offence under section 204A of the Penal Code 1871 (for obstructing, preventing, perverting or defeating the course of justice).

To share legally privileged material without inadvertent waiver of privilege, targets in an investigation may rely on the common law doctrine of common interest privilege to communicate legally privileged materials to each other. Under this doctrine, Party B, the recipient of privileged material from Party A, can resist disclosure of the legally privileged material provided by Party A on the ground that the material is subject to Party A's legal professional privilege.

To establish common interest privilege between Parties A and B:

- there must be common interest between Parties A and B in the outcome of the litigation or investigation;
- the document to be protected by common interest privilege must already be protected by Party A's legal advice privilege or Party A's litigation privilege at the time it is disclosed;
- the information to be protected must be confidential in nature; and
- the exchange or transmission of privileged documents must be for the purpose of furthering Party A and Party B's common interest.

Sharing of privileged material pursuant to the common interest privilege doctrine is not without risks; such risks include the possibility of inadvertent waiver of privilege through loss of confidentiality owing to more parties having access to or possession of such material, and Party A potentially losing the ability to assert legal privilege as against Party B in subsequent proceedings if their interests were to diverge.

Law stated - 2 July 2025

Investor notification

20 At what stage must the target notify investors about the investigation? What should be considered in developing the content of those disclosures?

Generally, all companies listed with the Singapore Exchange (SGX) (ie, issuers) must continuously conduct self-assessments to determine whether a particular piece of information is material and requires disclosure to investors (via public announcement on SGXNet). The disclosure regime is intended to strike a fair balance between the need for continuous disclosure to investors of material information and the need to ensure that issuers are not unduly burdened by having to disclose every single piece of information, however trivial, that may be likely to have an effect – but not a material effect – on the price of their securities.

Subject to certain exceptions, it is necessary to disclose, on a timely basis, any information known to the issuer concerning it or any of its subsidiaries or associated companies that is either necessary to avoid the establishment of a false market in the issuer's securities or would be likely to materially affect the price or value of its securities (Rule 703 of SGX Mainboard Listing Rules).

Paragraph 8 of Appendix 7.1 of the Corporate Disclosure Policy (Appendix 7.1) cites common (non-exhaustive) examples in which the SGX would expect immediate disclosure,

including ‘an investigation on a director or an executive officer of the issuer’. The SGX’s Practice Note 7.1 Continuing Disclosure (Practice Note 7.1) provides further guidance on when disclosure should be made in the context of government investigations.

These guidelines should be taken into account in deciding on the stage at which an issuer must notify investors about the investigation. Where there is an investigation in respect of a director or an executive officer of the issuer, the following events are likely to require immediate disclosure (subject to satisfying the materiality requirement):

- the director or executive officer has been served with an order for the production of documents to assist in an investigation in relation to a breach of law, rule or regulation;
- the director or executive officer was investigated and interviewed by the relevant authority;
- the director or executive officer has surrendered their passport to a relevant authority, has been arrested (with or without posting bail) by a relevant authority or has been formally charged by a relevant authority, or a relevant authority has imposed conditions or restrictions on the director or executive officer; or
- the director or executive officer has been convicted or disqualified or is the subject of any judgment or ruling.

Similarly, where the issuer itself is involved in an investigation, the following events are likely to require immediate disclosure (subject to satisfying the materiality requirement):

- the issuer has been contacted by a relevant authority or served with an order for the production of documents to assist in an investigation in relation to a breach of law, rule or regulation; or
- the issuer has been informed or becomes aware that any of its subsidiaries or associated companies are under investigation by a relevant authority.

Depending on the factual circumstances, the disclosure obligation may be triggered at an earlier stage (if at all). If there is uncertainty, the SGX encourages issuers to err on the side of disclosure. Disclosure may be delayed or withheld only in limited circumstances, such as where the information is confidential, insufficiently definite, or disclosure would be misleading. These exceptions are narrowly construed and cease to apply once the information leaks to the media or market and becomes public.

In considering the content of a disclosure, an issuer should take into account paragraphs 5.11, 5.17 and 6 of Practice Note 7.1, as well as Part IX of Appendix 7.1. The SGX expects the issuer to set out, among other things:

- the relevant facts and details of any other conditions or restrictions imposed by the relevant authority (where applicable);
- the alleged offences and identity of the offender that the authorities were investigating, as stated in the order (where applicable); and
- the statement of the board of directors that it will continue to monitor the progress of the investigation and provide updates on material developments.

Where there may be a financial impact or other material consequence to the issuer, this should also be stated in the announcement; if the financial impact cannot be ascertained with certainty, the issuer should provide an explanation for the non-disclosure and sufficient information to enable investors to independently assess the impact, taking into consideration the variables disclosed.

Private companies are not subject to public market disclosure rules, but may still have notification obligations under financing arrangements, shareholder agreements or contractual covenants. These companies should carefully review their key agreements and consider whether counterparties may need to be informed, particularly where the investigation could impact operations, management or financial performance and trigger certain covenants.

Law stated - 2 July 2025

COOPERATION

Notification before investigation

21 Is there a mechanism by which a target business can cooperate with the investigation? Can a target notify the government of potential wrongdoing before a government investigation has started?

Yes, a target may notify the government of potential wrongdoing before an investigation has been commenced, for example, by contacting the relevant government entity directly.

There are also statutory mechanisms to notify the regulators, for example, suspicious transaction reports that are filed under section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA) when, among other matters, the company knows or has reasonable grounds to suspect that any property represents the proceeds of, or was used in connection with, criminal conduct (relating to, among other matters, offences set out in the Second Schedule to the CDSA, including fraud and corruption).

Certain regulated financial institutions are also required to lodge a police report and/or submit a misconduct report to the Monetary Authority of Singapore (MAS) within 14 days of discovery that a representative has engaged in specified misconduct — for example, where there is reason to suspect that the representative has committed fraud or dishonesty, or where the representative was involved in insider trading.

Law stated - 2 July 2025

Voluntary disclosure programmes

22 Do the principal government enforcement entities have formal voluntary disclosure programmes that can qualify a business for amnesty or reduced sanctions?

The majority of government enforcement entities do not have formal voluntary disclosure programmes, with the exception of the Competition and Consumer Commission of

Singapore, which maintains a leniency programme under which companies that come forward with information on cartel activity may be granted complete immunity or a reduction in financial penalties. The Inland Revenue Authority of Singapore also has a Voluntary Disclosure Programme, under which financial penalties may be reduced if voluntary disclosures meeting certain requirements are made.

While there may not be formal voluntary disclosure programmes in place, the general principle is that a business that voluntarily discloses potential wrongdoing to an enforcement agency would likely be treated with some leniency depending on the circumstances.

Law stated - 2 July 2025

Timing of cooperation

23 | Can a target business commence cooperation at any stage of the investigation?

Yes, a target business may generally commence cooperation at any stage of the investigation, although the extent to which credit is given for cooperation may vary. The earlier the stage at which the target business commences cooperation, the more credit is likely to be given.

Law stated - 2 July 2025

Cooperation requirements

24 | What is a target business generally required to do to fulfil its obligation to cooperate?

A target business should cooperate fully and promptly with the government entity's directions and requests (eg, for production of documents and information). The target may additionally undertake remedial measures and, where applicable, make restitution or disgorge the profits received from any misconduct.

Law stated - 2 July 2025

Employee requirements

25 | When a target business is cooperating, what can it require of its employees? Can it pay attorneys' fees for its employees? Can the government entity consider whether a business is paying employees' (or former employees') attorneys' fees in evaluating a target's cooperation?

As a matter of employment law, the company, as the employer, may request that its employees cooperate with an ongoing investigation commenced by the authorities, as such a request would generally be considered lawful and reasonable and an employee would have an implied obligation to comply with it. Such an obligation on the part of the

employee may also be set out in the employment contract and related human resources and investigation-related policies or procedures.

A company can decide to bear the legal fees for its employees who are assisting with the investigations involving the company, although there is generally no obligation for the company to do so. Such costs to the company may potentially be covered by the directors' and officers' liability insurance it has in place, if any. Unless the company's payment of legal fees incurred by its employees (or former employees) has a demonstrable effect on the extent of the information or evidence available to be provided to the investigating authority, it is unlikely that this would be considered a relevant factor in evaluating the company's degree of cooperation with the investigation.

Law stated - 2 July 2025

Why cooperate?

26 What considerations are relevant to an individual employee's decision whether to cooperate with a government investigation in this context? What legal protections, if any, does an employee have?

While individual employees may not have an express obligation under employment law to cooperate with the government investigation, they should carefully consider a reasonable request from the company to cooperate, as wilful disobedience may amount to a breach of an implied term of the employment contract to obey the employer's lawful and reasonable requests.

Where the request for cooperation is made not by the company but by the government agency conducting the investigation, in the lawful exercise of the agency's statutory powers, the employee is legally obliged to cooperate, and there may be sanctions for non-compliance.

Law stated - 2 July 2025

Privileged communications

27 How does cooperation affect the target business's ability to assert that certain documents and communications are privileged in other contexts, such as related civil litigation?

Sharing of privileged documents with the authorities (being a third party) may constitute a loss of confidentiality or waiver of privilege for the purposes of related civil litigation. Care should be taken to ensure that privileged documents are not shared with the authorities without an assessment of the potential implications for doing so, taking into account the potential safeguards and the ability to maintain privilege for the purposes of future legal proceedings. In litigation, if only a portion of privileged material is disclosed, there is a risk of wider waiver over other material that relates to the same subject matter.

Regulators may request a privilege waiver, although it is unclear what benefit may be obtained by the company from such waiver.

Companies should take care not to waive legal privilege when updating whistle-blowers and communicating with employees; they should consider preparing separate communications with more limited information as appropriate (eg, in connection with disciplinary proceedings).

Law stated - 2 July 2025

RESOLUTION

Resolution mechanisms

28 | What mechanisms are available to resolve a government investigation?

Criminal investigations may be resolved through mechanisms such as a guilty plea or a deferred prosecution agreement (DPA) instead of a criminal trial. Under a DPA, the Public Prosecutor agrees to defer prosecution of a corporation in exchange for strict compliance with certain conditions, which may include remediation efforts, the implementation of adequate compliance procedures and the appointment of a monitor.

Self-disclosure of violations is likely a factor the Public Prosecutor will consider when deciding whether to enter into a DPA with a company to resolve corporate misconduct under the DPA regime. DPAs were first introduced into Singapore's criminal justice framework through the Criminal Justice Reform Act 2018. In March 2024, it was announced that the Public Prosecutor is in discussions with a shipbuilding company on a DPA that will require the company to pay a proposed financial penalty of US$110 million for alleged corruption offences that occurred in Brazil. Subject to finalisation of the content and terms, and approval by the Singapore High Court, this would be Singapore's first DPA.

There are other potential outcomes, such as the issuance of a stern warning or a conditional stern warning (also referred to as a conditional warning) instead of prosecution, or compounding of the offence. Representations may be made to the Attorney-General's Chambers (AGC) at any stage to request such alternate outcomes, and the AGC has ultimate discretion whether to accede to or reject the requests.

An example of the use of conditional stern warnings can be seen in the enforcement action taken by the Corrupt Practices Investigation Bureau (CPIB) against a Singapore-based shipbuilding company in December 2017 as part of the company's global resolution with the US Department of Justice and the Brazilian and Singapore authorities. In announcing the resolution, the CPIB and the AGC stated that in issuing the conditional warning, due consideration was given to the company for self-reporting to the CPIB and the AGC the corrupt payments that had been made.

Where civil enforcement or regulatory actions are concerned, representations may generally also be made to the relevant enforcement agency to seek more lenient action in the interest of resolving the investigation. For example, in the case of a Monetary Authority of Singapore (MAS) civil penalty, the offender may enter into an out-of-court settlement

with MAS, under which the penalty amount may be less severe than if the civil penalty had been ordered by the court.

Law stated - 2 July 2025

Admission of wrongdoing

29 | Is an admission of wrongdoing by the target business required? Can that admission be used against the target in other contexts, such as related civil litigation?

An admission of wrongdoing is generally required where resolution mechanisms such as a guilty plea, a DPA or an out-of-court settlement are invoked. It is likely that such admission can be used against the target in other contexts, such as related civil litigation, particularly as the aforementioned resolution outcomes would usually be made public.

For example, in the context of an out-of-court settlement of a civil penalty, MAS has stated that the 'admission of liability is an important aspect of the settlement, as the reputational consequences that result from the admission can have a deterrent effect on the public'.

Where an investigation is resolved through other outcomes (eg, issuance of a stern warning or conditional stern warning instead of prosecution), an admission of wrongdoing is typically required, although it is not strictly necessary.

Law stated - 2 July 2025

Civil penalties

30 | What civil penalties can be imposed on businesses?

The primary civil penalty that can be imposed on companies is a financial penalty. The range of the penalty depends on the applicable legislative provision. For example, under section 232 of the Securities and Futures Act 2001, the financial penalty may not exceed three times the amount of profit gained or the loss avoided as a result of the contravention or S$2 million (whichever is greater), and must not be less than S$100,000.

Where MAS is concerned, other types of enforcement action include revocation or suspension of the financial institution's regulatory status, directions to remove directors and officers, compositions, issuance of prohibition orders, reprimands, warnings or letters of advice.

Law stated - 2 July 2025

Criminal penalties

31 | What criminal penalties can be imposed on businesses?

Criminal penalties in the form of fines can be imposed on businesses. The range of the fine depends on the applicable legislative provision. For example, under the Prevention of Corruption Act 1960, the maximum fine that can be imposed on a business for conviction on a charge of corruption is S$100,000. Generally, companies can only be subject to a fine if they are found guilty of a criminal offence under the relevant legislation.

Regarding individuals within the company (eg, directors and employees), other criminal penalties such as imprisonment, fines and disqualification of directors may be imposed on the individuals.

Law stated - 2 July 2025

Sentencing regime

32 | What is the applicable sentencing regime for businesses?

Sentencing depends on the relevant offence committed and the specific facts of each case. All sentences ordered by the court must be within the types and range of punishment as provided by the relevant legislation. The sentence to be imposed will be determined by the judge, who will generally consider the company's culpability, the harm caused by the offence and applicable aggravating and mitigating factors.

Case law continues to shape the sentencing regime for corporate misconduct. For example, in *Goh Ngak Eng v Public Prosecutor*[2023] 4 SLR 1385, the High Court introduced a structured sentencing framework for private sector corruption offences under sections 6(a) and 6(b) of the Prevention of Corruption Act 1960. The High Court set out, among other things, offence-specific factors for determining harm (such as the extent of loss to third parties, public disquiet, or involvement of transnational elements) and culpability (such as planning, sophistication and abuse of position and breach of trust).

More recently, in *Public Prosecutor v Zheng Jia* [2025] SGHC 76(*Zheng Jia*), the High Court adopted a separate framework for sentencing breaches of directors' duties under section 157(1) of the Companies Act. There, a chartered accountant who acted as a nominee director of companies incorporated for foreign clients admitted to registering these companies and opening related bank accounts without exercising any oversight over the affairs of the companies. Two of these companies were found to have processed proceeds of scams perpetrated abroad. A district judge imposed fines, but the High Court overturned the fines and imposed consecutive prison terms totalling 10 months.

The High Court decisively moved away from the previous benchmark set in *Abdul Ghani bin Tahir v Public Prosecutor* [2017] 4 SLR 1153, which had reserved imprisonment for intentional or reckless breaches. Instead, *Zheng Jia* introduced a three step sentencing framework for breaches under section 157(1) of the Companies Act, which includes a consideration of offence specific factors such as a failure to monitor transactions, profit driven misconduct, duration of the breach and involvement of any transnational elements.

These decisions together highlight the growing judicial emphasis on corporate accountability in Singapore.

Law stated - 2 July 2025

Future participation

33 What does an admission of wrongdoing mean for the business's future participation in particular ventures or industries?

This depends on the nature of the wrongdoing, the business and the industry. For example, where financial institutions are concerned, the Monetary Authority of Singapore (MAS) can withdraw its approval of a financial institution if it appears that, among other matters, it is in the public interest to do so (section 4(5) of the Financial Services and Markets Act 2022).

MAS has exercised such power when it found instances of serious misconduct on the part of the financial institution. For example, in 2017, in connection with a high-profile grand corruption scandal in an Asian country involving fund flows into certain banks in Singapore, MAS shut down two merchant banks owing to 'egregious failures of [anti-money laundering] controls and improper conduct by senior management'.

Where public sector contracts are concerned, the Standing Committee on Debarment (SCOD) decides whether to debar companies from participation in government contracts. The grounds for debarment have been published on the government's e-procurement portal, GeBIZ. The Corrupt Practices Investigation Bureau may recommend a contractor to the SCOD for debarment action where, for instance, it is established that the contractor or any of its employees, directors, etc, had bribed a public sector officer or another person in connection with a government agency or contract.

Similarly, where the Competition and Consumer Commission of Singapore (CCCS) has issued an infringement decision finding that two or more contractors had engaged in bid-rigging in connection with a government tender, the CCCS may recommend to the SCOD that debarment action be taken.

Law stated - 2 July 2025

UPDATE AND TRENDS

Key developments of the past year

34 Are there any emerging trends or hot topics that may affect government investigations in your jurisdiction in the foreseeable future?

In the past year, Singapore has taken a series of coordinated measures aimed at strengthening enforcement against corporate misconduct, with a particular focus on money laundering. The 2024 Money Laundering National Risk Assessment identified the banking sector, including wealth management, as presenting the highest money laundering risk, followed by corporate service providers (CSPs) and digital payment token (DPT) service providers. The Monetary Authority of Singapore (MAS) echoed these findings in its latest Enforcement Report (July 2023–December 2024), identifying anti-money laundering and countering the financing of terrorism (AML/CFT) supervision and digital asset regulation as enforcement priorities for the year ahead.

Recent legislative reforms enhance enforcement while addressing these risks.

First, the Anti-Money Laundering and Other Matters Act 2024, partially effective November 2024, introduces significant amendments to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act to address evidentiary challenges in prosecuting complex, cross-border money laundering. A key amendment removes the requirement for the prosecution to link criminal property to a specific predicate offence. Prosecutors now need only show that the accused knew or had reason to believe the property was illicit, significantly easing the evidentiary burden in money laundering cases. The Act also expands the list of predicate offences to include foreign environmental crimes, such as illegal mining and wildlife trafficking. To improve detection of money laundering, terrorism financing and proliferation financing, the amendments further enable enhanced cross-agency data sharing between law enforcement and regulatory agencies and the Suspicious Transaction Reporting Office.

Second, the Corporate Service Providers Act 2024, effective June 2025, introduces a mandatory licensing regime for incorporation agents and nominee directors. CSPs will be subject to AML/CFT obligations and fit-and-proper criteria, and regulated by the Accounting and Corporate Regulatory Authority which can issue fines and disqualify individuals for violations. This reflects a broader trend towards gatekeeper accountability, holding intermediaries accountable as potential enablers of misconduct.

Third, the Financial Institutions (Miscellaneous Amendments) Act 2024, effective January 2025, harmonises and expands the MAS's enforcement powers across all statutes it administers. It authorises the MAS to enter premises without a warrant (and in some cases, without prior notice) and to compel information or interviews, including from former regulated individuals. The Act also facilitates evidence-sharing between the MAS, law enforcement and the Public Prosector for criminal investigations and proceedings.

Fourth, the Criminal Procedure (Miscellaneous Amendments) Act 2024, effective May 2025, among other things, empowers law enforcement agencies to conduct searches of premises without a warrant in specified circumstances and issue production orders for customer information held by financial institutions.

Fifth, under the Financial Services and Markets Act 2022, effective June 2025, all DPT service providers operating in or from Singapore must be licensed by 30 June 2025, even if serving only overseas clients. The MAS has set a high bar for licensing and will generally not approve applications from DPT service providers whose substantive regulated activities occur outside Singapore, given the higher money laundering risks and the MAS's limited ability to supervise such entities effectively.

In November 2024, the MAS also confirmed it would formally regulate Single Family Offices (SFOs) under a new class exemption regime. Under the rules, SFOs must be wholly owned by family members (either directly or via family-controlled entities), maintain an account with an MAS-regulated financial institution responsible for performing AML/CFT checks, declare any investigations or legal proceedings involving family members, and file annual reports. This follows a 2023 consultation and addresses growing concerns about the role of SFOs in facilitating illicit asset flows.

Finally, the National Asset Recovery Strategy, published in June 2024, reinforces asset recovery as one of the key pillars of Singapore's AML regime. It establishes a whole-of-government task force to coordinate asset tracing, seizure, forfeiture and

repatriation across agencies including the MAS, CAD, CPIB and AGC, and encourages joint investigations and multi-agency case planning to streamline recovery.

Law stated - 2 July 2025

NORTON ROSE FULBRIGHT

Wilson Ang	wilson.ang@nortonrosefulbright.com
Jeremy Lua	jeremy.lua@nortonrosefulbright.com
Charis Low	charis.low@nortonrosefulbright.com
Chen Yan Wang	chenyan.wang@nortonrosefulbright.com
Terence De Silva	terence.desilva@nortonrosefulbright.com

Norton Rose Fulbright

Read more from this firm on Lexology