

International Comparative Legal Guides

Corporate Investigations 2026

A practical cross-border resource to inform legal minds

10th Edition

Contributing Editor:

Michael Diamant

Gibson, Dunn & Crutcher LLP



iclg

Expert Analysis Chapters

1

Navigating Attorney-Client Privilege and Work Product Protection in Corporate Investigations

Michael Diamant, Melissa Farrar, Monica Limeng Woolley & Ben Schlichting, Gibson, Dunn & Crutcher LLP

10

Asia-Pacific Overview

Dennis Miralis, Jasmina Ceic, Kartia Zappavigna & Jack Dennis, Nyman Gibson Miralis

Q&A Chapters

21

CanadaIris Fischer, Liam Kelley & Cate White,
Blake, Cassels & Graydon LLP

29

England & WalesTom McNeill, Richard Reichman, John Binns &
Anoushka Warlow, BCL Solicitors LLP

38

FinlandMarkus Kokko, Vilma Haavisto & Matti Teräväinen,
Borenium Attorneys Ltd

44

GermanyChristian Pelz, Maximilian Ohrloff, Ingo Theusinger &
Zoé Flöer, Noerr Partnerschaftsgesellschaft mbB

51

GreeceIlias G. Anagnostopoulos & Padelis V. Bratis,
Anagnostopoulos

57

ItalyRaffaella Quintana, Ornella Belfiori, Francesca Cannata &
Paolo Vespa, ADVANT Nctm

65

MalaysiaJack Yow, Kwong Chiew Ee & Penny Wong Sook Kuan,
Rahmat Lim & Partners

73

NorwayElisabeth Roscher, Tine Elisabeth Vigmostad,
Geir Sviggum & Kristin Nordland Brattli, Wikborg Rein

81

PortugalBárbara Marinho e Pinto & Lua Mota Santos,
Rogério Alves & Associados

90

SingaporeThong Chee Kun, Jansen Chow, Josephine Chee &
Jason Lim, Rajah & Tann Singapore LLP

98

SwitzerlandDr. Daniel Lengauer, Dr. Michael Daphinoff,
Dr. Roman Huber & Cristina Ess, Kellerhals Carrard

108

TaiwanMichael T. H. Yang & Edward T. C. Wen,
Lee and Li, Attorneys-at-Law

115

USAMichael Diamant, Melissa Farrar, Lora MacDonald &
Todd Truesdale, Gibson, Dunn & Crutcher LLP

Italy

Raffaella
QuintanaOrnella
BelfioriFrancesca
CannataPaolo
Vespa

ADVANT Nctm

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 obligations or with regulatory expectations? Are there any regulatory or legal benefits to conducting an investigation?

In Italy, internal investigations conducted by in-house functions are not legally privileged. In contrast, if entities want to conduct privileged “defensive” investigations, these shall be carried out by the appointed defence counsel. In the Italian legal system, defensive investigations can be carried out both in cases where a criminal proceeding is already pending, as well as before the start of the criminal trial (so-called “*preventive*” defensive investigations). With respect to defensive investigations in general, Italian law provides for specific procedural and legal safeguards, mandated mainly by the Code of Criminal Procedure¹ (“**ICCP**”) and by the Ethical rules on the processing of personal data for defensive investigations issued by the Italian Data Protection Authority (Act no. 512/2018).²

In addition to that, in general terms, all corporate investigations shall be conducted within the framework of the Workers’ Statute (Law 300/70³) and the Italian Privacy Code (Legislative Decree 196/2003⁴), along with the GDPR.⁵

For the sake of completeness, it should also be noted that, at the international level, *ISO 37008:2023 – Internal Investigations of Organizations – Guidance* (“**ISO 37008**”) provide for a globally recognised framework for planning, conducting and reporting internal investigations. Although not legally binding under Italian law, adherence to the principles and best practices set out in ISO 37008, without prejudice to the application of any relevant legal provision, may further demonstrate an entity’s commitment to compliance.

Violation of the relevant legal provisions may result, depending on the case, both in the lack of legal privilege over the findings of the investigation and/or in the imposition of administrative or, in serious cases, criminal sanctions.

While Italian law does not provide direct legal benefits to entities for conducting an investigation, a proactive approach in addressing potential misconducts generally demonstrates a “good citizenship” attitude and ethical business culture. In any case, from a more practical perspective, such an approach enables companies to gather valuable information that can guide the definition of their defensive strategy before enforcement authorities.

For instance, in criminal proceedings involving legal entities under Legislative Decree 231/2001⁶ (“**231 Decree**”, providing for corporate criminal liability), the findings of internal investigations may play a crucial role in identifying appropriate remedial actions, which can, in turn, be recognised as mitigating circumstances when sanctions are determined. By way of example, if an investigation leads to the elimination of the harmful effects of the misconduct, compensation for damages, or the adoption of an Organisation, Management and Control Model under the 231 Decree (the “**231 Model**”), such actions may mitigate liability and reduce potential penalties.

1.2 How should an entity assess the credibility of a whistleblower’s complaint and determine whether an internal investigation is appropriate? Are there any legal implications that should be kept in mind while dealing with whistleblowers?

The assessment of the credibility of a whistleblower’s complaint is part of the management process of the latter (ISO 37008, in this regard, recommends that – where possible – the investigation team should engage with the whistleblower to obtain additional details in relation to the allegations, thereby enabling a more accurate and well-documented assessment of his/her credibility).

When determining whether a follow-up internal investigation is appropriate, entities may want to give priority to investigating those facts that could compromise their reputation and/or could give rise to, most notably, corporate criminal liability.

In any case, entities dealing with whistleblowers shall act in compliance with Legislative Decree 24/2023⁷ (“**WB Decree**”), according to which, unless they report or disclose false information intentionally or with gross negligence, whistleblowers are entitled to significant protections (e.g. non-retaliation, confidentiality, limitations of liability) and to specific timeframes safeguarding their reporting rights (e.g. for the notice of receipt of the report and its feedback).

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 should outside counsel take to ensure that the reporting relationship is not compromised by internal conflicts? When is it appropriate to exclude from participation in the investigation company personnel such as an in-house

attorney, senior executive, or major shareholder who might have a conflict of interest *vis-à-vis* the investigation?

As anticipated, privileged “defensive” investigations shall be carried out by the appointed defence counsel. Such an appointment can only be made, on behalf of the legal entity, by individuals granted with the appropriate powers to do so (e.g. Chairman of the Board of Directors, with powers of legal representation of the company).

To ensure that the reporting relationship is not compromised by conflict of interest, the first step for the appointed defence counsel is to clearly determine who the findings should be reported to. In this regard, in general terms, findings should be ordinarily reported to the person who appointed the defence counsel. However, in practice, situations may arise where that individual may, also just potentially, be involved in the facts to be further investigated internally. For this reason, it is crucial to understand how powers of attorney and delegations are formalised, and to ensure in any case that the findings are also reported to an investigation team that should preferably include control functions, such as Audit and Compliance.

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 an internal investigation? What factors do they consider in this regard?

In contrast to the approach of other (mainly common law) jurisdictions, Italy’s legal system does not generally provide for voluntary disclosure regimes. Hence, the primary practical function and value of conducting defensive internal investigations lies in granting the entity with the opportunity to gather information/evidence useful for defining the most appropriate defensive strategy and/or for potential defence in court proceedings.

For the sake of completeness, however, for certain corruption offences, Italian law provides for an incentive mechanism (which directly impacts on possible sanctions) in case of effective adoption of steps to secure evidence and to ensure the identification of the individuals responsible for the crime.

2.2 Assuming that an entity has determined that disclosure of an internal investigation is appropriate, what factors should corporate counsel consider as regards when and how to make such a disclosure to enforcement authorities?

Entities may freely choose which parts of the privileged investigation to disclose, as sharing selected findings is allowed.

In any case, even when opting to disclose only a portion of the findings of the investigation, all potential consequences should be carefully assessed, both from a legal and a reputational perspective. Indeed, amongst others, since criminal prosecution is mandatory in Italy, disclosure may – under certain circumstances – lead to the initiation of proceedings not only for the violations initially investigated internally, but also for any other violations that the authorities may deem relevant (including for corporate criminal liability under the 231 Decree).

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

While the ICCP provides for specific formalities for some activities carried out during defensive investigations (e.g. technical analyses, interviews; see, in particular, question 7.1), no particular requirements are imposed regarding the formalisation of the findings of the investigation.

However, a full and secure control over the circulation of written reports is a matter of utmost importance. Accordingly, the decision to draft a written investigation report must strike a balance between, on the one hand, the need to formalise the outcomes of the investigation and, on the other, the necessity to preserve legal privilege and confidentiality.

3 Cooperation with Law Enforcement Authorities

3.1 If an entity is aware that it may be the subject or target of a government investigation, must it or should it liaise with local authorities before starting or progressing an internal investigation?

There is no legal obligation in Italy to liaise with the Public Prosecutor before starting/progressing a defensive investigation. Whether to do so should be evaluated on a case-by-case basis.

In particular, on one hand, engaging with the Public Prosecutor may help the company to better understand the main areas of interest for the prosecution and, consequently, allow it to define the scope of its internal investigation more effectively. On the other hand, however, informing the authorities of the company’s intention to conduct an internal investigation may draw additional (and perhaps unwanted) attention to the facts under scrutiny.

3.2 If regulatory or law enforcement authorities are investigating an entity’s conduct, might the entity have the opportunity to influence the scope of a government investigation? If so, what objectives should the entity pursue, how are those best achieved, and what are the risks, if any?

In Italy, it is not possible to directly influence the scope of a criminal investigation, though there are, depending on the stage of the proceedings, procedural instruments available to the persons or entities under investigation to exercise their right of defence (e.g. the submission of defensive briefs aimed at presenting new facts/a different reconstruction of the facts or offering a different legal interpretation of facts already under investigation).

In broad terms, it shall also be noted that criminal investigations are generally subject to secrecy; therefore, an individual/entity may become aware of its involvement in criminal proceedings even years after their commencement, when the Prosecutor’s investigation is concluded.

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

Italian Public Prosecutors seem to increasingly coordinate

with authorities in other jurisdictions, especially within the European Union (“EU”). In this area, cooperation mechanisms have been strengthened through institutional bodies and agencies, such as the European Public Prosecutor’s Office, Eurojust and Europol, which facilitate the exchange of intelligence and evidence in cross-border investigations and the set-up of joint investigation teams (“JITs”).

Even more, when entities face investigations in different jurisdictions, it is advisable to convene a multijurisdictional team of defence counsel to ensure a full and consistent understanding of all legal implications at hand.

4 The Investigation Process

4.1 What steps should corporate counsel typically consider when putting together an investigation plan?

A comprehensive investigation plan should include some or all the following steps: *i*) appointment of external counsel to preserve the legal privilege on the activities (see question 4.2); *ii*) setting up of an investigation team (see question 1.3); *iii*) definition of the investigation scope of work, having regard – *inter alia* – to the potential legal, operational and reputational risks or challenges that the subject matter of the investigation may pose to the entity; *iv*) appointment and coordination of technical experts, with the expertise required by the case (see question 5.2); *v*) preservation of evidence, possibly also through legal hold notices/IT back end holds, and secure data collection procedures (see question 6.1); *vi*) preliminary document analysis; *vii*) forensic activities on corporate devices and review of items selected by means of search-terms; *viii*) interviews with individuals possibly having useful information for the reconstruction of the facts (see questions 7.1ff.); *ix*) reporting the findings to the client (see question 2.2); and *x*) proposed remedial actions.

In relation to point *iii*), it should also be underlined that the scope of the investigation should be regarded as part of an ongoing and dynamic process. For instance, ISO 37008 specifically recommends that the investigation scope should be promptly adapted when the investigation team becomes aware of additional alleged misconduct or illicit activities.

4.2 When should companies engage the assistance of outside counsel or outside resources such as forensic consultants? If appropriate to engage outside counsel or other resources, what criteria or credentials should companies consider in making their selection(s)?

Under Italian law, the involvement of outside counsel is necessary to preserve legal privilege over the findings of the investigation (see questions 1.1 and 5.1). Such a choice also depends on the nature of the allegations and on the facts under scrutiny. By way of example, for sensitive issues, and, most notably, for those that could possibly lead to corporate criminal liability or, in any case, expose the company to serious reputational risks or damages, ensuring legal privilege to the investigation’s activities and findings would be certainly relevant.

Additionally, if the facts under scrutiny involve multiple jurisdictions and require different expertise, it is advisable to set up a multijurisdictional and/or multi-practice team for the defensive investigation activities.

Depending on the strategy adopted, the technical complexity of the issues beneath the facts under scrutiny, and the nature of the activities within the scope of work (which may, for instance, involve forensic activities or technical evaluations of the investigated circumstances), companies may

also engage technical experts (e.g. in the IT, scientific, medical fields, etc.). To maintain legal privilege over their activities, experts should be formally appointed by the external counsel before the start of their activities.

5 Confidentiality and Attorney-Client Privileges

5.1 Does your jurisdiction recognise the attorney-client privilege, attorney work product doctrine, or any other legal protections relevant to internal investigations? What best practices should be followed to preserve these protections?

In Italy, legal privilege entails that the investigation activities and related findings remain at the exclusive disposal of the Company and its defence counsel, who may also decide not to disclose them to public Authorities.

In order to achieve such protection, Italian law requires that the investigation activities are conducted by a defence counsel appointed to this end and that all formalities provided by the ICCP are followed (e.g. specific warning to interviewees, formal minutes of technical operations and interviews, etc.).

In addition, practical tips to preserve legal privilege include, amongst others: *i*) using secure channels for document exchange; *ii*) including clear disclaimers on communications/documents to alert potential external readers that the content is confidential and protected by legal privilege; and *iii*) copying external counsel on all communications regarding the investigation.

5.2 How do legal privileges or work-product protections apply to interactions between a client and third parties engaged by outside counsel during an internal investigation (e.g. an accounting firm engaged to perform transaction testing or a document collection vendor)?

In order to extend the legal privilege to the consultants’ activities and findings, technical experts shall be formally appointed by the external defence counsel before the start of their activities. Confidentiality obligations also apply to them and remain in effect after the conclusion of the technical assignments.

5.3 Does the application of legal privileges or other work-product protections vary in your jurisdiction based on whether in-house counsel or outside counsel direct an internal investigation?

Yes. In Italy, legal privilege does not extend to activities solely conducted by in-house counsel.

5.4 How can entities best protect privileged or work-product protected records during an internal investigation conducted in your jurisdiction?

See question 5.1.

5.5 How do enforcement agencies in your jurisdiction treat the confidentiality of the results of an internal investigation voluntarily provided by the entity?

In cases of disclosure to the Public Prosecutor, legal privilege on what is disclosed is waived. The related documents/reports

become part of the criminal case file and are therefore subject to the confidentiality rules applicable to criminal proceedings.

6 Data Collection and Data Privacy Issues

6.1 How do data protection laws or regulations impact internal investigations in your jurisdiction?

Data protection laws and regulations (see question 1.1) should be duly considered while conducting internal investigations in Italy. This means that, both prior to and throughout the investigative activities, company policies/procedures shall be carefully examined – for instance, to verify whether employees have been properly informed of the types of activities the entity may perform and for what purposes the company’s devices could be used (i.e. whether mixed-use of corporate devices is allowed or not and whether a minimum retention period is provided for company laptops used by pre-identified personnel of sensitive positions after the personnel leave the organisation, as suggested by ISO 37008).

In particular, for instance, compliance with this category of regulations implies that only data that are strictly necessary for the investigation’s purposes can be processed, and that access to such data shall be limited to the appointed defence counsel and authorised individuals (e.g. consultants, collaborators of the defence counsel).

Data protection laws and regulations also have a significant impact on the transfer of documents and data in cross-border matters, especially if extra-EU.

Lastly, when AI systems are used to assist in document review, data analysis, or evidence classification, particular care must be taken to verify whether the use of AI is compliant with data privacy/protection, by way of example with respect to the modalities in which the data provided are stored, as well as whether the latter are reused to train the AI tool.

6.2 Is it a common practice or a legal requirement in your jurisdiction to prepare and issue a records preservation notice to individuals who may have materials 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 in the notice? How should compliance with the preservation notice be recorded?

It is not a legal requirement to prepare and issue a records preservation notice. When deciding whether to do so, entities should weigh both the potential advantages (e.g. evidence preservation and possibility of taking disciplinary actions against those employees who intentionally violate the legal hold) and disadvantages (e.g. potential disclosure of the existence of the investigation).

That said, when drafting a legal hold, it is essential to balance safeguarding data integrity with maintaining confidentiality over the investigation’s scope. Accordingly, the list of recipients and the scope of the documents or data covered by the hold letter should be determined on a case-by-case basis, ensuring that the specific facts under scrutiny in the investigation are not disclosed, while still providing sufficient clarity for the interested employees to understand which (and what kind of) data/documents/materials should be preserved.

Compliance with the preservation notice by employees could be formalised by requiring them to sign an acknowledgment form confirming their understanding. For the sake

of completeness, we highlight that breaches of the hold letter may also be relevant under a disciplinary perspective.

As an alternative to a legal hold, entities may also consider implementing an “IT hold”, which technically prevents the deletion, overwriting, or alteration of items on company servers or devices without requiring explicit communication to individual employees.

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

In this case, the entity shall ensure compliance with all local applicable laws (e.g. bank secrecy laws, data privacy – see question 6.1, procedural requirements, labour laws). For instance, as anticipated above, the location of the servers relevant for forensic activities may have a significant impact on the applicable legal framework, particularly in light of the rules governing data transfer.

6.4 What types of records do enforcement agencies in your jurisdiction typically consider important for collection in the context of an internal investigation?

In the context of criminal investigations conducted by Public Prosecutors, inspections and seizures may be carried out, during which all corporate documents deemed relevant to the criminal case are typically seized.

For instance, in cases of bid rigging, the authorities will generally collect tender documentation, relevant contracts and corporate procedures. They may also acquire the company’s 231 Model (if any), together with the minutes of the Supervisory Body established under the 231 Decree, as well as any risk assessment document.

Therefore, in the case of an internal investigation, the appointed defence counsel should first collect and analyse all documents that have been acquired or are, in any case, of possible interest for the authorities. Additionally, the counsel should gather and analyse any other data/material useful for the reconstruction of the facts under scrutiny, also in view of the definition of the defensive strategy and/or the defence of the entity, if any.

6.5 What resources do corporate counsel typically recommend to efficiently collect records relevant to an internal investigation?

To efficiently collect records relevant to an internal investigation, it is generally advisable to use virtual rooms, which ensure secure data exchange. The e-mails and related attachments relevant for the investigations are also stored within dedicated review platforms, provided that the use of such tools is included in the investigation plan (see also question 6.7).

6.6 How are predictive coding techniques typically viewed by judicial or enforcement authorities in your jurisdiction?

In Italy, the debate around the use of predictive coding techniques remains relatively underdeveloped at the level of enforcement agencies. In general terms, however, when authorities are faced with innovative tools, they tend to focus

on analysing whether their use (e.g. for document review activities) complies with applicable laws and principles (e.g. maintenance of the chain of custody), as well as whether the resort to such methodologies and tools and related next steps are properly documented.

See question 6.7 for our experience.

6.7 What best practices are utilised to efficiently review voluminous records collections in internal investigations?

Best practices for an efficient review of voluminous records collections in internal investigation include: *i*) the complete digitalisation of the process, through a regularly updated online platform; *ii*) selection of relevant items by using keywords or AI prompts (on which, see also below) and a time-frame consistent with the facts under scrutiny (also taking into account data protection compliance requirements); and *iii*) the deployment of AI systems, which can be prompted to spot patterns of illicit conduct and/or explore specific topics.

In this regard, our team contributed to the development and lawyer-based training of an AI-enabled service designed to detect bribery and cartel risks in corporate contexts. Such system combined advanced machine learning and language processing techniques, to identify patterns and anomalies in vast amounts of textual data, supporting analysis in over 100 languages.

Furthermore, for forensic activities, our team regularly employs highly innovative digital platforms that combine technology-assisted review (“TAR”) and predictive coding techniques, allowing them – even within large datasets – to automatically mark relevant documents, learning from the decisions previously made by the reviewer, as well as to filter out relevant text passages from documents. In addition, such platforms allow the reviewer to dynamically interact with the AI tool through the drafting and submission of targeted user-friendly search prompts, thereby enabling a more adaptive review process that is progressively reshaping our working methodology in conducting defensive investigations.

7 Witness Interviews

7.1 What local laws or regulations might apply to interviews of employees, former employees, or third parties? What authorities, if any, should entities consider consulting or advising before initiating witness interviews?

If interviews are conducted with the formalities of defensive investigations, aimed at safeguarding legal privilege, the specific requirements provided for by the ICCP shall apply.

In particular, interviewees shall be sent written formal invitation with adequate notice before the interview takes place and, during the interview itself, the defence counsel appointed for the investigation by the entity must give him/her some warnings, including: *i*) the purpose of the interview; *ii*) duty to declare whether he/she is under investigation or charged in the same criminal proceeding (if any) or in related/connected proceedings; *iii*) right to remain silent; *iv*) duty of confidentiality regarding questions and answers made (also with respect to any questions made/answers given to the Prosecutor and *vice versa*, if applicable); and *v*) the potential criminal liability for false statements. The interview itself shall also be documented by drafting minutes, which must be signed by the

interviewee. Instead, if the interview is conducted remotely, the same is entirely recorded, and only summary minutes tracking the above-mentioned warnings are drafted.

During the interviews, witnesses have no statutory right to be assisted by a lawyer, unless they have been charged with a criminal offence in the very same criminal proceedings for which the investigation is being conducted, or in connected or related criminal proceedings. If that is the case, the witness must be accompanied by a lawyer, who shall also receive formal invitation before the interview.

Additionally, in cases involving specific offences (e.g. minor pornography), when gathering information from minors, the outside counsel shall seek the assistance of an expert in psychology or child psychiatry; at the same time, translators shall be involved in cases where the interviewee does not speak the same language as the defence counsel conducting the interview.

On the contrary, there is no obligation to notify a works council or other employee representative body about an internal fact-finding investigation.

7.2 Are employees required to cooperate with an internal investigation being conducted by their employer? When and under what circumstances might employees decline to participate in a witness interview?

Italian law does not provide any obligation on the employees to actively cooperate with the internal investigation.

In particular, if interviews are conducted with the formalities of defensive investigations, employees can decline to participate in the interview and, in general, they have the right to decide not to answer some or all questions made (however, if they decide to do so, they must tell the truth, otherwise they may be committing a crime; see also question 7.1).

That said, for the sake of completeness, please consider that companies’ codes of conducts may require employees to maintain a high level of cooperation, including in the context of internal investigations.

7.3 Is an entity required to provide legal representation to witnesses prior to interviews conducted as part of an internal investigation? If so, under what circumstances must an entity provide legal representation for witnesses?

No. See question 7.1.

7.4 What are best practices for conducting witness interviews in your jurisdiction in the context of an internal investigation?

In addition to the rules outlined in question 7.1, best practices also include: *i*) providing the interviewee with reasonable notice (usually, in practice, at least 24 hours) ahead of the meeting; *ii*) ensuring that the interview takes place in a dedicated space, with no persons present other than those authorised (such as defence counsel, any appointed technical expert, and the interviewee); *iii*) guaranteeing that interviews are carried out in the absence of any form of threat, promise, inducement or oppression; and *iv*) where minors are involved, ensuring the presence of an expert in psychology or child psychiatry in all cases to provide appropriate support.

7.5 What cultural factors should interviewers be sensitive to when conducting interviews in your jurisdiction in the context of an internal investigation?

Cultural factors should be carefully considered depending, amongst others, on the allegations involved, the nationality and cultural identity of the interviewee, as well as the nature/scope of the investigation. For instance, in cases involving sensitive issues such as sexual harassment in workplaces, particular attention should be paid to cultural norms and communication styles that may affect how questions are perceived and answered. For instance, ISO 37008 recommends that, in certain cultural or geographical contexts, if the interviewee is a woman, it may be appropriate to include a female member within the interviewer's panel.

7.6 When interviewing a whistleblower, what considerations can an entity take into account to protect the interests of the company while respecting the rights of the whistleblower?

When interviewing a whistleblower, the entity should carefully balance the protection of the whistleblower's rights (e.g. confidentiality and non-retaliation) with the company's legitimate interest in effectively investigating the reported facts and reconstructing potential responsibilities.

7.7 In your jurisdiction, do employees have any right to review or revise statements they have made in the context of an internal investigation?

As noted above, if interviews are conducted with the formalities of defensive investigations, employees are not obliged to answer questions but, if they decide to do so, they must tell the truth. That said, even if interviewees are not granted a copy of the minutes of the meeting with the appointed defence counsel, they shall have the opportunity to read/revise their statements prior to signing, in order to ensure that the minutes accurately reflect what was actually said. In case of interviews that are entirely recorded, because conducted remotely, the recording itself constitutes the official record, and only summary minutes with the warnings required by the law are drafted.

7.8 Is there any requirement in your jurisdiction that enforcement authorities or a witness' personal legal representative be present during witness interviews conducted in connection with an internal investigation?

As noted above, the presence of a witness' defence counsel during the interview is generally not provided for. However, such presence becomes mandatory when the interviewees have been charged with a criminal offence in the very same criminal proceeding for which the investigation is being conducted, or in a connected or related criminal proceeding (see also question 7.1).

In contrast, no enforcement authorities can participate to the witness interviews. In this regard, please note that, in Italy, defensive investigations conducted by an appointed defence counsel follow a completely different path from those carried out by the Public Prosecutor.

Accordingly, as anticipated (see question 7.1), before proceeding with a witness interview, the interviewee must be informed, amongst others, of the prohibition on disclosing any

questions that may have been asked by the Public Prosecutor or law enforcement officers delegated by the latter, as well as the answers provided. It is worth noting that such prohibition of disclosing questions made/answers given also applies in the opposite case, namely when the witness is heard by the Public Prosecutor and has already been interviewed by the defence counsel in the context of defensive investigations.

8 Investigation Report

8.1 How should an investigation report be structured and what topics should it address? Under what circumstances should a company consider instructing the preparation of a formal written report?

While there are no legal requirements regarding the investigation report, it is advisable that it may include: *i*) an executive summary, outlining in a few points the key findings and conclusions; *ii*) description of the background and scope of the investigation; *iii*) description of the steps and activities undertaken (including, where possible, relevant figures and data – e.g. list of custodians, search terms and/or AI prompts list, number of items hit by the launched search terms for the purposes of document review, and/or any other outcome of the technical experts' activities, etc.); *iv*) findings and related assessment based on external legal frameworks (e.g. Criminal Code, 231 Decree) and internal rules (corporate procedures, disciplinary system, ethical code, etc.); *v*) list of proposed remedial actions (e.g. disciplinary measures, compliance programme self-assessment, review of corporate procedures, media statement); and *vi*) a section addressing any other issue (if any), namely covering any matter that, while initially outside the scope of the investigation, nevertheless emerged as potentially relevant.

With regard to whether the investigation report should be in written form, it is advisable that the decision should be made based on the specifics of the case and allegations. For further considerations, see question 2.3.

9 Trends and Reform

9.1 Is it possible to see how corporate investigations tend to correlate to active government enforcement in your jurisdiction? If so, what lessons can be taken from activity in recent years?

In recent years, criminal seizure of devices, servers and other digital data has increased, particularly in the case of large-scale investigations, such as those involving offences against the Public Administration (e.g. bribery and corruption, bid rigging). The same applies to tax-related offences, in which the Tax Authority typically exercises broad powers that are substantially similar to those of Public Prosecutors.

In this context, it is particularly relevant for entities to adopt a proactive approach, in order to proceed as soon as possible with the reconstruction of the facts and, subsequently, anticipating and addressing any potential misconducts and/or weaknesses in their internal control systems.

9.2 What enforcement trends do you currently see in your jurisdiction?

In Italy, current enforcement trends mainly regard:

- i. irregularities in the supply chain, leading to the commencement of criminal proceedings, also against legal entities, for the offence of unlawful exploitation of labour, particularly within the fashion sector. These cases have repeatedly led to the imposition of court-appointed judicial receivers (*amministratori giudiziari*);
- ii. corruption-related offences, including in relation to major public or private investments, with particular regard to, *inter alia*, the real estate and infrastructure sectors;
- iii. tax crimes, also in relation to cross-border tax fraud; and
- iv. enforcement of international sanctions, also following the adoption of EU Directive 1226/2024, which sets to criminalise the violations of EU restrictive measures, and which Italy has very recently taken steps to implement through Draft Legislative Decree 317/2025, introducing liability for both individuals and legal entities.

9.3 What (if any) changes in enforcement do you see on the horizon?

In Italy, enforcement activities may be expected to evolve in the close future due to the growing influence of technology, particularly in the areas of cybercrime and AI.

Moreover, the application of AI tools within enforcement and judicial systems, if adopted, is likely to speed up processes that are currently slow and resource intensive.

In this regard, in some foreign jurisdictions, AI systems are already embedded with various law enforcement functions. US agencies, for instance, regularly use AI for supporting their missions (e.g. the Department of Homeland Security employs systems that analyse data to enhance border security and assess risks in immigration processing).

In Italy and other jurisdictions, however, structured AI programmes have not yet been integrated within the Public Prosecutors' activities. Nonetheless, some sector-specific and/or pilot initiatives have already emerged.

The Italian Financial Intelligence Unit, for instance, very recently published a draft regulation containing new guidelines for detecting and reporting suspicious transactions,

which signals an openness to using AI-based systems to identify anomalous operations.

With respect to the Italian administration of justice, an application interface based on AI is already technically available to Judges and Public Prosecutors. However, its use within judicial activities is currently restricted to a very limited number of experimental programmes expressly authorised by the Ministry of Justice, for exploratory purposes only. By contrast, its application is permitted for activities within the justice sector that do not have a material impact on the outcome of any decision-making process (e.g. organisational management, preparation of statistical reports, graphic design, language revision, etc.).

In any case, discussions are currently ongoing as to the development within the Italian justice system of an internal AI platform – hosted on ministerial servers or locally – dedicated to supporting judicial and administrative functions in a secure and compliant manner.

Endnotes

- 1 ICCP (https://www.gazzettaufficiale.it/dettaglio/codici/codiceProceduraPenale/326_0_1).
- 2 Italian Data Protection Authority, Act no. 512/2018 (<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9069653>).
- 3 Law 20 May 1970, no. 300 (<https://www.gazzettaufficiale.it/eli/id/1970/05/27/070U0300/sg>).
- 4 Legislative Decree 30 June 2003, no. 196 (https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218).
- 5 Regulation (EU) 2016/679 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504>).
- 6 Legislative Decree 8 June 2001, no. 231 (<https://www.gazzettaufficiale.it/eli/id/2001/06/19/001G0293/sg>).
- 7 Legislative Decree 10 March 2023, no. 24 (<https://www.gazzettaufficiale.it/eli/id/2023/03/15/23G00032/sg>).



Raffaella Quintana is the Head and Coordinator of the White Collar Crime, Investigations & Compliance department at ADVANT Nctm. She deals with all issues related to corporate criminal law, with particular regard to cases of corruption, fraud, tax, corporate and financial offences, as well as aspects related to the liability of entities pursuant to Legislative Decree no. 231/2001.

She defends directors and managers of national and multinational companies in criminal proceedings arising from their activities in the company, as well as companies involved in proceedings pursuant to Legislative Decree no. 231/2001.

She provides assistance in compliance matters, including the preparation of compliance programmes and internal control systems for large corporations and multinational groups under domestic and foreign law (UK Bribery Act, FCPA) and has extensive experience in conducting defensive investigations, including coordinating multidisciplinary and cross-border teams of professionals.

ADVANT Nctm

Via delle Quattro Fontane, no. 161
00184 Rome – RM
Italy

Tel: +39 06 6784977

Email: raffaella.quintana@advant-nctm.com

LinkedIn: www.linkedin.com/in/raffaella-quintana-74635923



Ornella Belfiori is a Senior Associate in the White Collar Crime, Investigations & Compliance department at ADVANT Nctm.

Ornella provides practical, day-to-day advice on trade compliance issues of all varieties. She is particularly skilled in creating successful strategies for handling economic sanctions adopted, amongst others, by the European Union and OFAC, as well as export controls regimes. She frequently counsels clients in connection with custom-related product classifications and supports them in liaising with competent Authorities to obtain relevant licences and authorisations.

She regularly advises clients in international enforcement matters, including those arising under the FCPA and other anti-bribery legislations. She gained substantial experience in handling cross-border internal investigations across a broad range of topics including, among others, bribery and corruption, fraud, bankruptcy and tax crimes.

ADVANT Nctm

Via delle Quattro Fontane, no. 161
00184 Rome – RM
Italy

Tel: +39 06 6784977

Email: ornella.belfiori@advant-nctm.com

LinkedIn: www.linkedin.com/in/ornellabelfiori



Francesca Cannata is a Senior Associate in the White Collar Crime, Investigations & Compliance department at ADVANT Nctm. She has nearly eight years of experience in providing both judicial and extra-judicial legal advice to individuals and leading multinational and domestic companies with reference to criminal law and other compliance-related matters, with a specific focus on corporate criminal liability (Italian Legislative Decree 231/2001).

Francesca regularly participates in the defence of companies and top managers involved in criminal proceedings related to any kind of business activities, and has extensive experience in planning and conducting privileged defensive investigations (also preventive ones).

ADVANT Nctm

Via delle Quattro Fontane, no. 161
00184 Rome – RM
Italy

Tel: +39 06 6784977

Email: francesca.cannata@advant-nctm.com

LinkedIn: www.linkedin.com/in/francesca-cannata-2a74b194



Paolo Vespa is a Trainee Lawyer in the White Collar Crime, Investigations & Compliance department at ADVANT Nctm. He supports the team in advising Italian and international companies on matters of corporate criminal law, including the defence of directors and managers in proceedings arising from their professional activities.

He has gained experience within the conduction of defensive and internal investigations, including those with cross-border elements.

He is also actively involved in the design and implementation of Organisation, Management and Control Models pursuant to Legislative Decree 231/2001 as well as in broader advisory work on compliance and corporate governance matters, including supporting 231 Supervisory Bodies established pursuant to same Decree.

ADVANT Nctm

Via delle Quattro Fontane, no. 161
00184 Rome – RM
Italy

Tel: +39 06 6784977

Email: paolo.vespa@advant-nctm.com

LinkedIn: www.linkedin.com/in/paolovespa

ADVANT Nctm is the Italian member firm of ADVANT, a distinctly European association of independent law firms focused on helping clients navigate the complex and nuanced legal and commercial landscape of Europe. With around 360 professionals, including 85 partners and five offices in Italy and abroad (Milan, Rome, Genoa, London and Shanghai), ADVANT Nctm is one of the leading independent Italian law firms.

www.advant-nctm.com

ADVANT Nctm



The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Corporate Investigations 2026 features two expert analysis chapters and 13 Q&A jurisdiction chapters covering key issues, including:

- The Decision to Conduct an Internal Investigation
- Self-Disclosure to Enforcement Authorities
- Cooperation with Law Enforcement Authorities
- The Investigation Process
- Confidentiality and Attorney-Client Privileges
- Data Collection and Data Privacy Issues
- Witness Interviews
- Investigation Report
- Trends and Reform