Internal investigations: a roadmap for organizations

Transformative Legal Experts

PLMJ

Contents

1. What does it mean?

The term ‘internal investigations’ has become an increasingly common part of organisational vocabulary. This is driven by two main factors. The first is legislative developments in recent years across a wide range of areas, such as (i) fighting corruption, financial fraud and money laundering; (ii) tackling harassment and discrimination; (iii) regulating lobbying activities aimed at public decision-makers; (iv) improving data governance and information security; and (v) responding to personal data breaches and cybersecurity incidents. The second factor is growing institutional and reputational concerns in the face of various highly public cases of companies and individuals being held accountable for unlawful or unethical actions within their organisations.

Regardless of whether they are driven by legal obligation, moral imperative or reputational concerns, the fact remains that the most well-prepared organisations can no longer avoid investigating any suspicious incidents brought to their attention. Prudent organisations have already realised that this is an essential preventive tool.

Internal investigations are very common and have a long history in other jurisdictions, and they are growing in popularity here. They play a central role in the legal health of any organisation and in preventing or mitigating the liability of companies and their stakeholders.

We have therefore conducted an initial examination of the subject and its associated challenges and merits.

The first challenge is to define what an internal investigation is.

It is often easier to define something by what it is not than by its own characteristics. To a certain extent, this description fits internal investigations. This makes them easier to understand than the far better-known external investigations conducted by public bodies such as the police, tax authorities, public prosecutors and regulators and supervisory bodies.

External investigations are research and examination activities initiated by entities outside the organisation. They aim to establish facts and allegations in order to potentially determine the liability of various parties for legal, regulatory, or ethical breaches. Internal investigations involve the same process of fact-finding, but are driven by the organisation itself, which could potentially be the target of an external investigation.

Essentially, it is a process of verification and self-analysis carried out by the organisation regarding its own actions, procedures, and conduct within its structure, or by employees or third parties in its immediate vicinity, for example, suppliers in the supply chain. They must therefore play a central role in compliance processes, ensuring integrity and enforcing the law, as well as the organisation’s own policies and regulations.

While they can be carried out using in-house resources, it is common to engage external consultants or experts. Acting on behalf of the organisation that commissions them, these consultants or experts conduct impartial and technically rigorous investigations – without which they would lose their usefulness.

It is a process of verification and self-analysis carried out by the organisation regarding its own actions, procedures, and conduct within its structure, or by employees or third parties in its immediate vicinity,

In Portugal, however, internal investigations remain a neglected aspect of business and legal practice. This is due to various factors, such as cost and a lack of structures equipped to conduct them, but above all a lack of awareness of their strategic value.

Nevertheless, legal, institutional and reputational demands are placing internal investigations at the forefront of organisations' concerns. They are seen not only as a compliance tool, but also as a means of self-awareness and of preventing or mitigating the organisation's own liability, while also defending its governing bodies and strategic decision-makers.

Until recently, internal investigations merely followed external investigations, such as police searches or regulatory inspections. However, a new paradigm has now emerged: the autonomous internal investigation. These are used as a means of prevention, to hold offenders to account, and to ensure compliance. The aim is to prevent or stop any action that violates the law, best practice, or the organisation's own rules and principles.

Our exploration of this topic merely contributes to the practice of investigation within organisations, the relevance of which is becoming increasingly evident. This is only the beginning of a body of work that will constantly evolve and be refined.

2. Legal and institutional environment

The development of various legal instruments requiring organisations to conduct internal investigations has been one of the main drivers of this practice.

Organisations are now legally compelled to have adequate internal resources in place, either because they have an explicit legal obligation to conduct an internal investigation or because they are required to adopt mechanisms that encourage whistleblowing. Where such resources are lacking, organisations must seek specialist external support to ensure the effective conduct of investigations.

At the same time, the institutional and regulatory environment has become increasingly demanding. Several factors have established these investigations as an important management and control tool. These include protecting corporate reputation as a sign of good practice, and creating – and, in some cases, mandatorily establishing – compliance departments. Another factor is the growing interest in verifying compliance with internal policies, particularly within more complex corporate structures.

Firstly, we will briefly examine the legal and institutional factors that most frequently lead to external investigations.

2.1. WHISTLEBLOWING

Strengthening internal reporting systems is one of the main drivers of internal investigations. Organisations are required to set up secure reporting channels and clear triage procedures, as well as defined deadlines for following up on reports.

In Portugal, Law 93/2021, which transposes Directive (EU) 2019/1937, has established a detailed framework for the protection of whistleblowers. It requires public bodies and a wide range of private entities to establish internal reporting systems. These channels must ensure the confidentiality of the whistleblower's identity, as well as that of any third parties mentioned, and they must prevent any acts of retaliation. They must also comply with procedural deadlines (e.g. acknowledgement of receipt and provision of feedback) when handling reports.

Providing reporting channels alone is not enough. Effective compliance with these rules also requires the material and methodological capacity to impartially and effectively investigate the reported facts, in order to ensure the principles set out above are applied. In practice, this means that organisations must plan and conduct internal investigations to a high standard. They must define the scope of investigations, preserve evidence and establish risk matrices and materiality criteria. They must also document decisions and any limitations.

2.2. EMPLOYERS' HARASSMENT PREVENTION OBLIGATIONS

Since 2017, Article 127(1)(l) of the Labour Code has required the initiation of disciplinary proceedings whenever cases of alleged harassment are reported.

The law refers to a disciplinary procedure which not only requires the identification of the accused, but also the identification and specific attribution of the facts in question. This could suggest that employers are only obliged to act if they are provided with concrete and almost complete knowledge of all these circumstances, effectively placing them in a passive position.

However, an overall analysis of the employer's duties leads us to conclude that they have a duty to act diligently and proactively. Employers are required to investigate serious allegations of harassment that provide a minimum number of credible details, even if these details are still vague or not fully substantiated.

In 2017, the legislature also adopted a general prohibition on harassment, thereby strengthening the legal framework for this offence and its censure in the workplace. This clarified the right to compensation for harassed employees and expressly granted protection to complainants and witnesses in the event of a complaint regarding such behaviour.

Taken together with the duty of good faith in performing obligations and the duty to provide appropriate physical and moral working conditions, these elements lead to a clear conclusion. Employers must investigate allegations of harassment that are not manifestly unfounded. Where appropriate, this may require the use of a preliminary investigation procedure suited to the complaint submitted.

Therefore, whenever an employer receives complaints of harassment or descriptions of situations that may constitute harassment, they have a genuine duty to investigate such allegations diligently and impartially.

To prevent harassment, the legislature has also imposed an obligation to adopt a manual of good practice and harassment prevention under Article 127(1)(k).

This educational obligation is intended to enable employees to recognise and report unacceptable behaviour, whether affecting them directly or brought to their attention. Consequently, by fostering the reporting of abusive practices, it requires companies to carry out an increasing number of internal investigations in this area.

2.3. RGPC - GENERAL ANTI-CORRUPTION FRAMEWORK

The consolidation of cross-cutting regulatory frameworks for the prevention of corruption and related offences has introduced new requirements for risk assessment, as well as for the implementation of controls and continuous monitoring. This has a direct impact on the need to incorporate internal investigations into the integrity system.

Indeed, Decree-Law 109-E/2021 approved the General Anti-Corruption Framework (RGPC) and established an institutional framework, including the National Anti-Corruption Mechanism (MENAC). This requires entities covered by the law to adopt compliance programmes that coherently integrate risk assessment and mitigation plans and measures. They must also disseminate codes of conduct and policies for managing conflicts of interest, as well as a training plan and whistleblowing channels, all in line with Law 93/2021.

The existence of detection mechanisms – ranging from internal control alerts to whistleblowing reports – necessitates proportionate, technically supported, documented investigation methodologies that preserve the chain of custody and respect legal limits regarding labour matters and data protection.

Furthermore, at an institutional level, authorities with powers to apply penalties emphasise and value the robustness of the post-event response, the quality of the investigative process, and the effectiveness of corrective measures. Consequently, internal investigations conducted independently and consistently stand as an essential element of evidence for a culture of compliance and organisational diligence.

2.4. SECURITY INCIDENTS AND PERSONAL DATA BREACHES

Following security incidents, including those that qualify as personal data breaches under the GDPR, organisations must immediately assess whether an internal investigation is necessary. This is particularly necessary where there are indications of internal malicious conduct or non-compliance with policies and procedures. The investigation must be coordinated with the reporting obligations set out in the GDPR and relevant sector-specific and cross-cutting regulations. In particular, these include the NIS 2 Directive, which has been transposed into Portuguese law by Decree-Law 125/2025, and the DORA Regulation.

Where there are indications of internal malicious acts or gross non-compliance with procedures, the investigation must combine technical forensic analysis with organisational and disciplinary analysis.

Even in the absence of evidence of malicious intent, the investigation must establish whether there has been a breach of policies or procedures and assess the impact, implementing appropriate corrective measures where necessary. Security incidents often trigger the need for a structured internal investigation to determine the causes, scope, and remedial measures. This investigation must be integrated into the incident response plan and involve the rapid activation of technical and legal teams.

Where there are indications of internal malicious acts or gross non-compliance with procedures, the investigation must combine technical forensic analysis with organisational and disciplinary analysis.

Furthermore, in incidents involving personal data or regulated sectors, the internal investigation informs decisions regarding notification to the relevant authorities and data subjects, the content of public communications and the definition of remedial actions. Following an incident, it is essential that there is a proper fact-finding process, as the underlying cause may persist and lead to further incidents with more serious consequences, particularly from an administrative and reputational perspective. There is also a risk of substantial financial losses to the company.

This issue is particularly pressing in the context of cybersecurity, as recent legislative changes mean it is now a central issue of governance and risk assessment, not merely a matter of technical implementation.

In this regard, internal investigations, whether following an incident or in the form of an audit – which is sometimes directly required by law – are essential tools.

2.5. FRAMEWORK FOR THE LEGITIMATE REPRESENTATION OF INTERESTS

The legitimate representation of interests is governed by Law 5-A/2026 of 28 January. This law establishes transparency rules applicable to private entities, both domestic and foreign, involved in the legitimate representation of interests. It introduces an additional dimension of scrutiny that teams responsible for conducting internal investigations cannot ignore.

Analysing interactions between the company and public authorities, particularly with regard to legislative or regulatory processes affecting the digital sector, may reveal conflicts of interest, the flow of inside information, or practices involving undue influence that intersect with the matters under investigation. In this regard, integrating compliance with the rules on the representation of interests into internal investigations is now an unavoidable requirement. This approach must also take into account the institutional and relational dimensions of business activity.

2.6. STRENGTHENING OF DUTIES OF CARE AND RISK MITIGATION

Regulators' more frequent, vigilant and sophisticated approach across multiple sectors has raised the expected standard for internal compliance verification. Regulators value control maturity, prompt failure rectification and informed cooperation, presupposing credible internal investigations properly planned and carried out by competent, autonomous teams. In sectors such as finance, energy, telecommunications, healthcare, transport and competition, as well as those covered by Decree-Law 125/2025, there is a heightened expectation to identify root causes, quantify impacts, define remediation plans and monitor their implementation. Transparent reporting to the supervisor and consistent documentary evidence are also required.

This regulatory tightening translates into a greater duty of care being required of organisations, raising the standard of diligence expected in preventing, detecting and responding to irregularities. At the same time, the tightening of penalty frameworks across multiple administrative offence regimes intensifies the financial and reputational exposure associated with compliance failures. This reinforces the incentive to adopt internal verification mechanisms.

Consequently, the absence of an investigation, or the poor conduct of an investigation due to bias, methodological shortcomings, or incomplete documentation, may lead to more severe penalties and reveal governance weaknesses. Conversely, swiftly conducting investigations with chain-of-custody documentation, impartial interviews and rigorous document analysis, and implementing corrective measures promptly, constitute mitigating factors in determining penalties and are an indicator of accountability to the regulator. Consistency between reports and documentation from internal investigations is an element of institutional credibility and regulatory trust in itself.

2.7. DEFENCE AGAINST CIVIL, CRIMINAL AND REPUTATIONAL LIABILITY

Internal investigations are also an effective means of protecting organisations. They have far-reaching implications for civil, administrative and criminal liability, as well as for protecting corporate reputation.

In matters relating to criminal and administrative offences, effective compliance programmes, cooperation in establishing the facts, and prompt redress of loss and damage are valued criteria when determining and grading penalties. Technically robust internal investigations with an appropriate scope and transparent documentation strengthen an organisation's position. Clarity regarding professional privilege and confidentiality, implementation of legal holds and appropriate segregation of sensitive information help protect the legal strategy and reduce procedural risks.

In employment and civil matters, the validity of measures depends on the lawfulness and proportionality of the evidence. This also depends on respect for fundamental rights, personality rights and data protection. Otherwise, the evidence may be excluded and compensatory obligations may arise. Consistency and traceability between the facts established, the decisions taken, and the corrective measures adopted are crucial for defence in court and for the robustness of disciplinary decisions.

Finally, consistency between policy and practice – reflected in the ability to establish facts, make evidence-based decisions and implement proportionate corrective measures – is at the heart of the reputational response. This signals to stakeholders and authorities a culture of integrity that mitigates present and future risks. Strategic communication based on documentation produced during internal investigations must be tailored to different audiences (e.g. employees, customers, markets and regulators) to demonstrate accountability without compromising legal positions.

Internal investigations are therefore increasingly being used to pursue the above-described objectives. They are also driving the need to recruit staff and establish specialised internal departments in this area, as well as increasing the use of external consultants dedicated to this field.

3. Types of internal investigations

The need to launch an internal investigation may arise from various sources, including whistleblower reports, compliance alerts and proceedings initiated by regulatory bodies.

Similarly, the scope of a forensic investigation may cover issues such as breaches of internal procedures, ethical conflicts of interest (internal or within the supply chain), fraudulent practices, criminal offences and regulatory breaches, as well as workplace-related complaints.

Furthermore, the scope of the investigation may vary depending on the parties involved, distinguishing between employees, service providers, suppliers, partners, board members and customers.

Any of these approaches may necessitate a different classification of existing types of investigation. There is a profusion of different categorisation proposals and classifications of varying complexity. However, we believe that a functional and pragmatic approach should be prioritised. This classification should be practice-oriented and based on the required areas of specialisation, as this has been proven to be more effective:

- **Investigations into the workplace and working environment**, which focus on human behaviour and organisational culture.
- **Compliance and fraud investigations**, which ensure compliance with the law, regulations, and internal policies.
- **Corporate security investigations**, which protect the organisation's assets and operations.
- **Personal data breach and cybersecurity investigations**, which analyse cyber threats and data protection.
- **Digital compliance investigations**, which are cross-cutting and multidisciplinary by nature. For example, the implementation of a service based on artificial intelligence may cover risks related to personal data breaches and protection, cybersecurity vulnerabilities, algorithmic biases that could lead to unlawful discrimination or harm consumers, and financial or reputational risks to the organisation itself.
- **Government and regulatory investigations** aim to prevent or mitigate organisations' public, criminal and civil liabilities, as well as other reputational and social issues.

Rather than being of purely theoretical interest, this division enables a common approach across the different categories, bringing together concerns of a similar nature within each group and the experts most familiar with each type.

However, it should be noted that this is a constantly evolving landscape, requiring investigators to be highly adaptable. Investigations that were once rare may now be indispensable due to legislative changes, such as the emerging supply chain verification obligation under Directive (EU) 2024/1760. Therefore, the above classification will certainly evolve.

While this classification helps to structure investigative approaches, it is clear that investigations are not compartmentalised. They require a holistic view and multidisciplinary teams capable of achieving significant and effective results.

Different types of investigation require the investigative team to possess both specific expertise.

In practice, even if an investigation into suspected fraud is guided by the aim of preventing criminal liability, it is unlikely to dispense with a labour law analysis. The conduct in question may have been carried out by an internal agent, and their contract termination must comply with applicable labour rights. Similarly, an investigation into compliance with internal rules may require an assessment of corporate liability and the duties of care owed by directors. A competition law approach may also be required if there are infringements with potential competition implications.

In short, different types of investigation require the investigative team to possess both specific expertise and a cross-disciplinary perspective, enabling them to anticipate the need for cooperation with specialists from other fields.

4. Liability

Organisational liability lies at the intersection between the findings of an internal investigation and the potential legal, regulatory and reputational consequences resulting from them. As well as clarifying the duties and expected conduct of those involved, this chapter aims to explain how diligently conducting an internal investigation and designing it well can influence the company's position. It also examines how an organisation's response to an investigation's findings may either improve or worsen its standing with employees, the authorities, regulators, investors, and other stakeholders. We focus on demonstrating when there is a duty to investigate, the risks of non-compliance, the parameters that define the liability of legal persons and how directors' and other senior management's liability is structured.

4.1. LIABILITY FOR BREACH OF THE DUTY TO CONDUCT AN INTERNAL INVESTIGATION

In some circumstances, launching an internal investigation is not only advisable, but also legally required. Failure to fulfil this duty, even if no underlying misconduct is ultimately proven, may result in administrative liability.

This applies to a failure to fulfil the duty to investigate in the context of whistleblowing and harassment complaints, as mentioned above. Furthermore, various authorities in regulated sectors require incidents relating to compliance, cybersecurity, workplace conduct, market integrity or data protection to be subject to consistent internal investigations and reporting where applicable. Failure to investigate may reveal shortcomings in governance and internal control, which could trigger specific penalty proceedings and impact the assessment of the suitability and adequacy of management and supervisory bodies.

Beyond the framework for penalties, breaching the duty to investigate may strengthen the causal link in civil liability claims for failing to fulfil preventive duties, particularly where inaction allows harmful conduct to continue or recur. Conversely, a timely, robust investigation with proportionate solutions tends to mitigate exposure and demonstrate organisational diligence.

4.2. CORPORATE LIABILITY: PARAMETERS, MITIGATION AND AGGRAVATING FACTORS

A legal entity's liability generally arises from employment and regulatory offences committed within the organisation, criminal offences attributable to it under the law, and contractual or non-contractual breaches. Internal investigations play a dual role in all these areas: they serve as a diagnostic tool and as a means of assessing organisational culpability or due diligence.

In the criminal sphere, liability of a legal entity is determined by specific legal requirements relating to the actions of bodies, representatives or individuals acting on its behalf and to its benefit. When determining the applicable penalty, the relevance of prior compliance measures and the adoption of corrective measures following the detection of offences is becoming increasingly important.

In this context, the rules for determining penalties applicable to legal persons are particularly relevant. These rules value the existence and implementation of compliance programmes, the entity's cooperation in establishing the facts and the reparation of damages.

Consequently, conducting a credible internal investigation, using the established facts, and sharing the obtained evidence with the authorities generally has a mitigating effect on the penalty. The same applies to the swift implementation of solutions arising from the investigation's recommendations.

In the context of administrative offences, regulators tend to take into account the organisation's compliance culture, the effectiveness of its internal controls, its voluntary reporting, its cooperation, and its promptness in rectifying failures.

Superficial internal investigations aimed at confirming preconceived hypotheses, or those that disregard methodological limitations, may exacerbate the perception of risk and lead to heavier penalties. In contrast, well-defined procedures involving a preserved chain of custody, impartial interviews, rigorous document analysis and clear documentation of limitations reinforce the organisation's credibility and support the mitigation of penalties.

In employment matters, the quality of the investigation influences the robustness of disciplinary measures and the company's defence in litigation. Decisions based on unlawful evidence or evidence obtained in breach of personal rights and data protection are likely to be overturned by the courts, with consequences in terms of compensation and reputation. Adherence to the principles of proportionality, minimisation and transparency in the use of monitoring technologies, as well as respect for the limitations on remote surveillance and access to communications, is crucial for the validity of the results.

In civil matters, the company may be held liable for damages arising from the acts of its employees, contractors or management bodies where there has been a breach of duties of prevention or supervision. Clear policies, appropriate training, investigative diligence and effective remedial action are all factors that are taken into account when assessing organisational wrongdoing and liability. For example, this applies when determining compensation for wrongful dismissal, where the court is granted a margin of discretion based, among other factors, on the gravity of the employer's conduct.

Finally, comparative experience highlights the value of formalising compliance programmes involving periodic risk assessments, reliable whistleblowing mechanisms and internal investigation protocols. When applied in Portugal, these elements have been important in determining the level of potential fines and in adopting less onerous alternative measures. This is particularly the case where the law allows for post-facto conduct to be considered that demonstrates a genuine commitment to compliance on the part of the organisation.

4.3. LIABILITY OF INDIVIDUALS: DIRECTORS, MANAGERS AND OFFICERS

The liability of individuals in management roles and governing bodies runs parallel to that of the company and can be invoked at various levels. In corporate terms, directors are bound by duties of care and loyalty. They must ensure that internal control and risk management systems exist and function effectively, including mechanisms for detecting and investigating irregularities. Failure to fulfil these duties negligently may result in civil liability towards the company, its creditors and, in certain circumstances, third parties.

Directors and managers may also be held liable for specific administrative offences arising from organisational and control failures. In certain legal contexts, they may also be held liable for criminal offences committed in the course of their duties. Authorities frequently scrutinise certain factors as indicators of a culture of compliance and individual accountability. These include how management responds to warning signs, authorises internal investigations, allocates adequate resources, prevents undue interference, and implements recommendations.

The transposition of the NIS2 Directive into Portuguese law, effected by Decree-Law 125/2025, represented a paradigm shift in the way Portuguese organisations view cybersecurity. Until then, cyber risk management was often treated as a purely technical matter confined to information technology departments.

Decree-Law 125/2025 requires directors and senior management not only to approve cybersecurity risk management measures, but also to ensure their effective implementation to guarantee the organisation's operational resilience. Strictly speaking, this constitutes a genuine duty of supervision and due diligence for members of management bodies. They cannot simply delegate all security decisions to technical staff. Instead, they must take an active role in mitigating cyber risks. If the entity commits an infringement through an act or omission attributable to a management body member, that individual may be held personally liable under the terms of the legislation. As previously mentioned, the era in which cybersecurity and data protection could be treated as purely technical matters has come to an end in Portugal.

In the field of digital platforms, the Digital Services Act (DSA) further reinforces this approach to accountability at the highest level of corporate governance. The DSA requires very large online platforms and search engines to appoint an independent compliance officer or set up a department with direct access to the board of directors. This body must ensure that the compliance officer or department has sufficient authority, resources, and autonomy to monitor compliance with the DSA's obligations. Under Article 41 of the DSA, the management body is also responsible for defining and overseeing governance mechanisms for managing systemic risks, preventing conflicts of interest when carrying out the compliance function and ensuring adequate resource allocation for risk management.

In short, whether in the context of personal data protection (GDPR), cybersecurity (NIS2), artificial intelligence, or the regulation of online content (DSA), there is a converging regulatory trend towards the direct accountability of boards of directors and executive officers for the digital compliance of their respective organisations.

Regulations such as NIS2 and the DSA explicitly codify this requirement, stipulating that senior management must take personal responsibility for risk management and compliance measures. The objective is clear: to foster a culture of compliance from the very top of the organisational structure, ensuring that digital governance issues receive the strategic attention they deserve. Undue interference in investigations, retaliation against whistleblowers or witnesses, destruction of evidence, and instructions to adopt illegal evidence-gathering practices may compromise the validity of the investigation and expose individuals to personal liability. Such actions may also expose individuals to personal liability.

Therefore, timely internal investigations are a necessary mechanism for defending decision-makers as individuals.

Ultimately, the corrective response must be proportionate and traceable, involving disciplinary measures when justified, procedural corrections, training, strengthened controls, and reporting to the competent authorities where required by law or advised by risk. The true criterion by which an organisation's accountability is assessed is increasingly consistency between what it promises in its policies and what it actually does when faced with an incident.

5. Evidence gathering

In the context of an internal investigation, a company or organisation does not possess the same powers as public investigative bodies. Therefore, it is essential to understand the limitations imposed on internal investigations in this area.

Professional oversight of the investigation is advisable to a large extent due to the need to gather evidence. A critical view must be taken of the evidence to be gathered and how it will be preserved so that it can ultimately be used in court, as well as the lawful means of access.

Using unlawful evidence can create complications and undermine the investigation's ultimate objective. This justifies our focus on this topic, taking a brief look at typical forms of evidence and the necessary precautions.

5.1. DOCUMENTS

Access to, and analysis of, documents in an internal investigation must be based on the principles of necessity, proportionality, and minimisation of interference. There must also be explicit documentation setting out the scope, assumptions and limitations of the investigation.

> Access to, and analysis of, documents in an internal investigation must be based on the principles of necessity, proportionality, and minimisation of interference.

Firstly, access to corporate repositories and to documentation handled by employees – including work files and professional communications – must be governed by clear internal policies that have been previously disclosed. A well-defined investigative rationale must also be in place to safeguard the proportionality of the means, internal transparency, compliance with data protection rules and, ultimately, the fundamental rights of those concerned. In particular, Articles 16 to 22 of the Labour Code protect the confidentiality rights of employees. Similarly, Article 34 of the Constitution of the Portuguese Republic protects the confidentiality of communications, and restrictions on this confidentiality are only permitted if courts intervene in accordance with the law, typically in criminal proceedings. However, this exception does not justify access to personal communications in internal investigations. Therefore, employers must only have access to professional emails and technical records that is strictly necessary, and this access must apply only to professional accounts or folders. This access must be regulated and communicated to employees in advance. The content of messages identified as personal must be excluded, while respecting the principles of the GDPR and Law 58/2019.

In the context of incident investigations, data collection must essentially balance technical and legal considerations. Access to work-related communications and technical records should be limited to what is necessary to confirm working hypotheses and mitigate risks, with any relevant evidence being preserved immediately.

Secondly, the selection and handling of documents must comply with the principles of integrity and chain of custody. This includes ensuring the traceability of who accessed the material, when, and for what purpose, as well as the segregation of content by levels of confidentiality. Using controlled repositories, access logs and privilege or confidentiality markings on sensitive materials reduces the risk of confidentiality breaches and evidence contamination. It is also advisable to define the data-retention and deletion rules applicable to the investigation from the outset.

Consistency between the documentation produced during the investigation and the information reported to decision-makers or authorities is essential for credibility.

Thirdly, certain classes of documents are subject to privilege rules that impose additional restrictions. Correspondence and memoranda produced in the context of legal advice must be protected by legal professional privilege. This privilege also extends to forensic specialists acting under the direction of lawyers, provided there are appropriate contractual arrangements in place and the recipients and scope are clearly defined. The investigative strategy should therefore include mechanisms to safeguard privilege. It should also define the different versions of the outputs to be produced (privileged and executive) to ensure substantive consistency without disclosing protected content.

Fourthly, as will be discussed below, collecting documents involving personal data requires strict adherence to data protection principles. These include minimisation, limitation of purpose and proportionality in the use of monitoring or search technologies over large bodies of documents. Documenting decisions, such as selection criteria, exclusions and materiality assessments, strengthens the legitimacy of the processing and the defensibility of the methodology before administrative authorities and courts.

Finally, consistency between the documentation produced during the investigation and the information reported to decision-makers or authorities is essential for credibility. Planning the document gathering process, which also applies to digital and testimonial sources, helps limit the scope to indispensable documents in each context. This approach avoids unnecessary intrusion and ensures that the evidence collected is reliable, reproducible, and useful for supporting corrective and accountability decisions.

5.2. PROTECTING PERSONAL DATA AND ACCESS TO EMPLOYEES' ELECTRONIC INFORMATION

A personal data protection assessment should precede any investigation, ensuring that the rights of data subjects are respected, particularly in light of the General Data Protection Regulation. Accordingly, access to professional email accounts, organisation-issued devices and cloud repositories must comply with strict necessity, proportionality and minimisation criteria. Access must take place within a framework of clear, previously disclosed internal policies. Particular emphasis should be placed on providing prior information that organisational resources should not be used for personal purposes, alongside clear rules on information storage.

Article 20 of the Labour Code expressly prohibits the use of remote surveillance tools for monitoring employee performance. However, this is not an absolute prohibition. Such tools may be admissible for specific purposes where they can be justified by the protection of persons and property, or by the particular requirements of the activity in question. A fundamental condition for their use as evidence is that they must not have been implemented for the purpose of monitoring work performance.

In a professional context, this limitation has led to extensive debate in case law on the admissibility of evidence such as CCTV footage, GPS data installed in vehicles, and in an international context, activity-logging software[iii].

Accordingly, access to email, devices, and cloud services must be based on previously communicated internal policies that clearly define permitted uses and access procedures. Such access must also be justified by a specific necessity that cannot be achieved through less intrusive means. Additionally, the investigation must be properly documented, with its scope defined in advance.

If this delicate balance is not observed, organisations often find themselves in awkward and embarrassing situations. For example, an organisation may be required to compensate an employee who is known to have stolen from the company, because a court has deemed the evidence of that conduct to be unlawful.

Evidence obtained unlawfully due to breaches of personality rights, data protection rules or limits on surveillance may render investigative findings unusable and increase an organisation's employment, administrative or civil liability.

5.3. USING AI IN EVIDENCE GATHERING AND ANALYSIS

Using artificial-intelligence tools in internal investigations can significantly speed up the search and screening of large volumes of data. However, robust safeguards and prior assessment are required, as there are limitations that must be respected.

In this context, the selection of such tools must, firstly, ensure that they are technically reliable and do not compromise the validity of the evidence. On the other hand, it is crucial to ensure that the rights of those involved are adequately respected, particularly with regard to the protection of personal data.

Human oversight is indispensable from the outset, as important decisions cannot be based exclusively on automated outputs. Accordingly, both the handling of evidence and subsequent decision-making must involve informed human intervention and be properly documented. This is an essential condition to ensure the methodological adequacy of the investigation and the future admissibility of the evidence.

In line with the General Data Protection Regulation, decisions based solely on automated processing are prohibited where results may produce legal effects or similarly significant effects on individuals. This applies unless a legally recognised exception exists and appropriate safeguards are in place, particularly human intervention.

In addition, the way the tools work must be explainable and, where necessary, auditable. Ideally, the principles of data protection by design and by default should be applied. This includes defining purposes and legal bases in advance, as well as appropriately parameterising search and collection criteria in accordance with the principle of proportionality.

Supplier selection is also important. Providers should be selected on the basis that they adhere to good practices regarding confidentiality, information security and data protection, and are contractually bound to comply with these obligations.

Accordingly, despite the significant utility of AI in internal investigations, careful review and documentation are required for the selection of the supplier and technology, the configuration of searches, and the handling of outputs. This is necessary to ensure lawful and technically sound action while respecting the rights of those involved.

5.4. CHAIN OF CUSTODY AND INTEGRITY OF DIGITAL EVIDENCE

Due to its nature, digital evidence is particularly susceptible to accidental or intentional alteration, contamination, and loss of context. For this reason, formal procedures must be adopted to preserve its authenticity, integrity and reliability from the moment it is collected until it is presented and evaluated.
The absence of such procedures may prevent the use of the evidence collected.

To avoid this, measures designed to ensure a robust and demonstrable chain of custody must be taken before the collection of digital evidence begins. This includes demonstrating that no alterations have occurred and documenting all operations carried out.

Wherever possible, collection and examination should be performed by forensic experts or under their direction and supported by technical reports describing the methods, tools and versions used, the parameters configured, and the logs generated.

6. Investigative interviews

Statements obtained in investigative interviews constitute a form of evidence that requires specific consideration. This is primarily because their reliability and usefulness depend directly on how the interview is conducted, including the techniques used, the interviewer's preparation, and the framework provided to the interviewee. The interviewee must also be protected against practices that may affect the voluntariness, truthfulness or integrity of their testimony, as they are a holder of rights.

The true importance of interviews is captured perfectly in the following words:

> *"Interviews remain such an essential part of most corporate investigations. It is important for those conducting an investigation to understand that whilst documentary evidence can provide the underlying facts of a case; it is often the account given by those who are spoken with which deliver the context and detail of what happened."*

A wide range of individuals may be required for interviews as part of an investigation. These may include whistleblowers, witnesses, those affected by the investigation, the subjects of the investigation, and even third parties external to the organisation. There is no fixed script for deciding who should be interviewed, nor is there a strict interview model or mandatory sequence to be followed.

Instead, interviews should be conducted in a way that is appropriate to the specific case. This implies allowing room for adaptation within each interview guide and within the overall interview plan, including the order in which interviews are conducted.

▲ RETURN HOME

What is essential is coherent and consistent prior preparation and planning. It is common practice to isolate and interview the whistleblower or the person who raised the concerns under investigation at an early stage. Potential subjects of the investigation are typically approached at a later stage, once the investigator has more detail, context and understanding of the environment in which the alleged facts occurred, and is familiar with the organisation, its structure and its methods.

Regardless of their role in the investigation, interviewees should be treated with respect, integrity, objectivity and fairness by investigators. Investigators should aim to obtain facts and details that bring them closer to the objectives of the investigation.

While it is useful for investigators to have an interview guide, it should not be rigid. It should not prevent the investigator from deviating from it or abandoning it altogether if circumstances require it. Nevertheless, the guide plays an important role in helping to focus questioning, ensuring that key lines of enquiry are not overlooked and maintaining consistency across interviews conducted by different investigators working on the same case.

Interviews must also be recorded. This is an important means of supporting the final report, safeguarding its integrity and ensuring it aligns with the reported facts.

Audio or video recording is possible and can facilitate the conduct of the interview while ensuring the integrity of what is said. However, this must always be transparently disclosed to the interviewee and their consent obtained. Investigators should not rely on recordings to the extent that they dispense with taking notes during the meeting, as these remain a valuable aid in drafting the report and a useful reference tool in its preparation.

7. Key stakeholders - forensic experts

7.1. WHO THEY ARE AND WHY THEY ARE INVOLVED

By their nature, effective internal investigations are multidisciplinary. As well as the legal and strategic direction provided by lawyers, forensic specialists and technical experts may also be involved. Their involvement brings technical rigour, speed, and reproducibility to the fact-finding process. The main profiles typically include:

- digital forensic experts, who are responsible for forensic extractions and for the preservation and analysis of media and data (e.g. emails, devices, logs, applications), while maintaining the chain of custody;
- IT and cybersecurity specialists, focused on systems architecture, event analysis, intrusion detection and vulnerability assessment;
- data analysts and e-discovery teams, who structure, filter and correlate large volumes of information by applying search criteria and analytical techniques;
- financial and accounting / forensic accounting experts, who reconstruct financial flows, test controls, quantify impacts and identify anomalous patterns;
- due diligence specialists who are responsible for the lawful collection of public information and mapping relationships;
- physical security and operations experts, where logistical issues or access considerations arise;
- sector-specific specialists (e.g. pharmaceuticals, energy or financial services) who can interpret evidence in light of regulatory and operational specifics.

The rationale for their involvement is to: (a) ensure the technical preservation of evidence and the reliability of results; (b) accelerate the collection and analysis of complex data, enabling informed decisions within short timeframes; (c) reinforce objectivity and methodological independence in the fact-finding process; (d) translate technical evidence into narratives that are intelligible to decision-makers and public authorities. All such work is designed and coordinated under the direction of lawyers. They define the scope, materiality thresholds, assumptions and limitations to ensure alignment with the legal and regulatory strategy.

7.2. PRIVILEGE AND CONFIDENTIALITY EXTENDING TO PARTNERS AND FORENSIC EXPERTS

Given the importance of lawyers' professional secrecy, it is necessary to address the confidentiality regime applicable to forensic specialists acting as partners to legal advisers conducting an internal investigation separately.

Where forensic specialists collaborate with lawyers to provide legal services of any kind and act under their guidance and control, they are bound by the lawyers' duty of professional secrecy. This is in accordance with Article 92(7) of the Portuguese Bar Association Statute. That obligation should be operationalised through engagement letters and confidentiality agreements which: (i) refer expressly to the legal framework governing professional secrecy; (ii) define the scope of the work and its intended recipients; (iii) ensure that any outputs produced are marked as privileged and/or confidential; (iv) segregate environments and implement access management controls; (v) establish rules on the chain of custody, data retention, and deletion.

In all scenarios, the circulation of information must adhere to the principle of necessity. This should involve controlled information repositories and access logging to mitigate the risk of confidentiality breaches and evidence contamination.

7.3. CRISIS MANAGEMENT, CONFLICTS OF INTEREST, AND INTERNAL AND EXTERNAL COMMUNICATION

Many investigations take place alongside crisis management, whether it is related to reputation, operations, regulations or cybersecurity. This often requires the coordinated involvement of communications agencies and public relations specialists.

They typically prepare statements, Q&A documents and key messaging lines, define spokespersons, provide media training, monitor traditional media and social networks, design communication plans for internal and external stakeholders, and support the timing and content of mandatory communications to regulators, markets and customers. The activity of these teams must align with the legal strategy and with the factual findings already established. This is essential to avoid premature disclosures, inconsistencies, or interference with the investigation.

Multidisciplinary coordination requires a clear governance model. This includes designating a lead counsel, an operational coordinator and a steering committee comprising representatives from legal, compliance, IT/cybersecurity, human resources, internal audit and communications. Approval processes for external communications must be established. There should also be escalation rules for critical decisions, a decision log, and a responsibility matrix that clearly allocates roles. In regulated or listed environments, it is particularly important to align the investigation with reporting obligations. These may include notifications to supervisory authorities, personal data breach notifications or disclosures of inside information. Consistency must be ensured between what is communicated and what is formally documented.

The genuinely multidisciplinary nature of investigations requires the integration of criminal and administrative offence perspectives, labour law, data protection and technical domains (forensics and IT), as well as financial, operational and reputational considerations. This integration translates into: (i) defining testable working hypotheses and success metrics; (ii) evidence-collection plans combining digital, documentary and testimonial sources; (iii) impact assessment and damage quantification; (iv) the design of technically feasible remediation measures; (v) preparing narratives and supporting materials tailored to different audiences, including management, employees, regulators and the market. Coordinating these dimensions in a disciplined manner strengthens the evidential basis of the investigation, reduces regulatory and penalty risk, and accelerates reputational recovery.

7.4. SCOPE

The range of participants involved in internal investigations, as listed above, may lead compliance directors and managers to anticipate financial costs that could make them appear prohibitively expensive.

However, the number of participants involved in an internal investigation, as well as its scope and level of complexity, must always be proportionate to its purpose and requirements.

From the outset, it is important to design a plan and define the scope and requirements of the investigation, without ruling out any unexpected issues that may arise during the investigative process. This should limit the unnecessary use of resources by tailoring participants' involvement to the type of investigation, its sensitivity and its relevance to the organisation.

▲ RETURN HOME

8. Final report

The final phase of an internal investigation is the production of the final report.

The final report should:

- describe the context and triggers of the investigation.
- det out the methodology, effective scope, and limitations (including legal, technological, and time constraints);
- list the investigative steps taken and the sources of evidence, with notes on the chain of custody and the selection criteria;
- present a factual chronology, evidence or issue maps, and the main findings, clearly distinguishing between facts, inferences, and conclusions;
- assess the credibility and consistency of statements and records;
- articulate the legal and regulatory implications, the breached standards, the residual risks, and the available courses of action. Where appropriate, different versions should be produced, such as privileged and executive versions. These should preserve confidentiality and legal privilege while ensuring that what is reported is consistent with what has been documented.

The final report should also include analyses of materiality and the evidentiary standard applied. It should expressly identify areas of remaining uncertainty and the assumptions used. Technical annexes, such as forensic reports, e-discovery outputs and accounting working papers, may be referenced and segregated with access controls and confidentiality markings.

The final report should also include analyses of materiality and the evidentiary standard applied.

Corrective measures should be aligned with the identified root causes and prioritised according to risk, effort, and impact. These measures typically unfold across three horizons:

- immediate remediation to stop misconduct and mitigate harm, such as revoking access rights, correcting system configurations, suspending contracts and notifying affected parties;
- structural corrections to processes and controls, such as segregation of duties, reinforcement of second-line functions, alert automation, policy reviews and targeted training;
- individual and organisational accountability (e.g. disciplinary measures, recovery of undue benefits, contractual claims and, where required, reporting to the relevant authorities).

Wherever possible, each action should have a clear target, deadline, acceptance criteria, effectiveness metrics and post-implementation testing plan. Periodic reports should be provided to the management body, and to internal audit and regulators where applicable. Functions and steps may be segregated so that the organisation can carry out parts of the plan in-house, such as reporting, setting metrics and monitoring implementation, even if fact-finding has been outsourced.

The implementation plan for corrective measures should provide for a monitoring committee, review cadences, progress indicators, dependency management, and assessment of residual risks. The effectiveness of the plan should be validated through independent testing (e.g. by the internal audit team), supported by documentary evidence of implementation and results. Adjustments should be made where objectives are not met. In listed or regulated environments, execution must align with market disclosure and supervisory reporting obligations to ensure consistency between internal metrics and externally reported indicators.

The corrective measures plan should provide actionable insights for the compliance system. This could include updating risk maps, revising whistleblowing triage criteria, enhancing investigation playbooks, strengthening due diligence and third-party management requirements, and integrating practical cases into training programmes. Internal communication, tailored to different audiences while respecting confidentiality and data protection requirements, helps to consolidate a culture of accountability and prevention.

A formal case closure document (close-out memo) should record the status of remediation actions, the results of effectiveness testing, approved internal policy changes, and points of contact with the relevant authorities. This provides evidence of organisational diligence towards stakeholders and regulators, closing the cycle.

A culture that values transparency, accountability and compliance reduces the incidence of misconduct and increases the organisation's capacity for early detection and effective response.

9. Organisational culture and business sustainability

Internal investigations are, and should be, a tool for fostering a healthy organisational environment and affirming a culture of responsibility and sustainability within a collective structure that ultimately aims to fulfil its social purpose indefinitely.

Organisational culture is therefore the primary operating system of any compliance programme. It is more than a set of formal policies; it is reflected in shared expectations, tangible incentives and observable day-to-day behaviours.

A culture that values transparency, accountability and compliance reduces the incidence of misconduct and increases the organisation's capacity for early detection and effective response. This cultural dimension is therefore critical for business sustainability. It protects value, reduces the costs of non-compliance, preserves the social licence to operate, and creates resilience in the face of adverse events.

Although difficult to quantify, it represents a significant challenge – and arguably the primary objective – of human resources and compliance departments. It is, in effect, the organisation's soft skill, with a substantial, albeit sometimes invisible, impact and return.

Broadly speaking, business sustainability depends on the ability to manage conduct, operational and reputational risks in a systematic and predictable manner. Well-designed and well-executed internal investigations function as an organisational learning mechanism. They drive continuous improvement cycles that strengthen the compliance culture. What is identified and corrected in a specific case must be translated into policies, controls and training. Otherwise, the organisation risks losing critical knowledge and repeating structural failures. It is the link between the 'micro' (the incident) and the 'macro' (the integrity system) that transforms an investigation into an investment in sustainability.

Leadership plays a decisive role in shaping organisational culture. The tone at the top, reflected in consistency between words and actions, establishes clear boundaries for acceptable conduct and lends legitimacy to reporting and investigative mechanisms. Equally important is the 'mood in the middle,' i.e. how middle management translates expectations into day-to-day priorities.

In practice, poorly designed commercial targets, reward systems and operational pressures that conflict with integrity standards can undermine any policy. Therefore, management should calibrate incentives, incorporate conduct metrics into performance evaluations, and demonstrate through action that risk prevention and remediation are inseparable from performance.

Internal trust is a central cultural asset. A virtuous cycle is created when there are credible whistleblowing channels, effective protection for whistleblowers, impartial investigations and proportionate responses, because employees then believe that "speaking up is worthwhile". Without this level of trust, information circulates informally or is suppressed altogether, which impairs the organisation's ability to anticipate and mitigate risks. The quality of the investigative process – including impartiality, clear methodologies, proper documentation and prudent communication – therefore indicates cultural maturity. When employees perceive that the organisation learns from errors rather than seeking scapegoats without establishing the facts, adherence to its declared values is reinforced.

Integrating ethics, compliance and strategy is another vital dimension of sustainability. Consistency requires conduct risks to be considered in strategic decision-making, partner selection and expansion into new markets. Matters such as third-party due diligence, conflicts of interest, sponsorships, hospitality and interactions with the public sector should be governed by clear, proportionate criteria that are applied uniformly. The 'lessons learned' discipline that arises from internal investigations should inform risk maps, mitigation plans and role-specific training, thereby ensuring cumulative organisational development.

Technology also influences culture and sustainability. Automating controls, conducting continuous data analysis and implementing early-warning systems can reduce reliance on whistleblowing and enhance preventive capacity while lowering costs. However, when adopting tools, proportionality, internal transparency and data protection principles must be respected. Otherwise, trust may erode. Combining technology with training based on real-world dilemmas, leadership role modelling and feedback mechanisms creates a cycle of detection, understanding and correction.

Organisational culture and business sustainability are measured by outcomes.

Ultimately, organisational culture and business sustainability are measured by outcomes, such as fewer recurring incidents, shorter detection and response times, effective corrective measures, and positive perceptions from key stakeholders, including employees, customers, regulators, and investors. Therefore, organisations should define culture and integrity indicators, monitor them regularly, and report on their evolution internally. When culture and investigative processes reinforce each other, companies can strengthen their resilience, protect their reputation and sustain long-term value creation.

Effective and cost-efficient internal investigations are essential for monitoring the implementation and respect of organisational culture at all levels.

Although the term 'investigation' is often associated with misconduct, the increased use of well-designed investigations of various kinds will reduce this negative connotation. Over time, internal investigations should be viewed simply as an important compliance tool for fostering a healthy, ethical and respectful environment for people, transactions, markets and the environment alike.

About PLMJ

→ Who we are

"PLMJ is the most organised firm and the most committed at doing things on schedule and to the time that is asked. They are the most up to date and one of most professional law offices that work with us."

CLIENT REFERENCE FROM CHAMBERS AND PARTNERS

About the Internal Investigations team

→ What we do

KEY CONTACTS

Marta Salgado Areias

Managing associate in the Technology, Media and Telecommunications practice

(+351) 913 628 099
marta.salgadoareias@plmj.pt

Pedro Rosa

Managing associate in the Employment and Labour practice

(+351) 917 967 756
pedro.rosa@plmj.pt

Raquel Cardoso Nunes

Managing associate in the Dispute Resolution practice

(+351) 918 840 319
raquel.cardosonunes@plmj.pt

▲ RETURN HOME

May 2026

PLMJ COLAB ANGOLA — MOZAMBIQUE — PORTUGAL

www.plmj.com