TECHNICAL SPECIFICATION

ISO/TS 37008

First edition
2023-07

Internal investigations of organizations — Guidance

Enquêtes internes des organisations — Recommandations

Reference number
ISO/TS 37008:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 309, *Governance of organizations*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Internal investigation is an integral part of organizational management. Internal investigation is a professional fact-finding process, initiated by or for an organization, to establish facts in relation to alleged or suspected wrongdoing, misconduct or noncompliance (such as bribery, fraudulent activities, harassment, violence or discrimination). Internal investigations enable an organization to:

— make informed decisions if laws, regulations, industry codes, internal policies, procedures, processes, corporate compliance policy and/or the organization's values and ethics have been breached;

— understand the cause(s) that lead to the above-mentioned breaches;

— determine if an allegation or concern is substantiated or unsubstantiated;

— assess the financial loss of an organization;

— mitigate liability of the organization and/or its management;

— put in place and implement the necessary mitigation measures to prevent similar conduct from occurring;

— strengthen the organization's compliance and ethics culture;

— make external reporting to relevant authorities (law enforcement, judicial bodies, regulators or other bodies prescribed by law or regulation) or relevant interested parties when necessary;

— make decisions on sanctions of management and/or employees and debarment of working with third parties involved in unethical conduct.

Civil actions, whistleblower reports and external investigations by regulators can be reasons for internal investigation as well so that the concerned organizations can find out what triggered the actions, reports and external investigations, then take appropriate measures.

Internal investigation is part of a compliance management system. This document can be used to help with the implementation of other standards such as ISO 37301, ISO 37001 and ISO 37002. It can also be a useful tool for an organization to identify risks. With risk clearly identified, an organization can analyse the root causes of noncompliance and design measures to control the risks.

Not having the capabilities to conduct internal investigations and/or failing to conduct internal investigations can have adverse effects on an organization such as compromising the effectiveness of the compliance management system, failing to protect its reputation, and failing to detect and counter wrongdoing.

This document provides guidance for organizations to implement internal investigations based on the following principles: independent, confidential, competent and professional, objective and impartial, and legal and lawful.

Figure 1 is a conceptual overview of the investigative process showing the whole picture of internal investigation and the possible post-investigation actions.

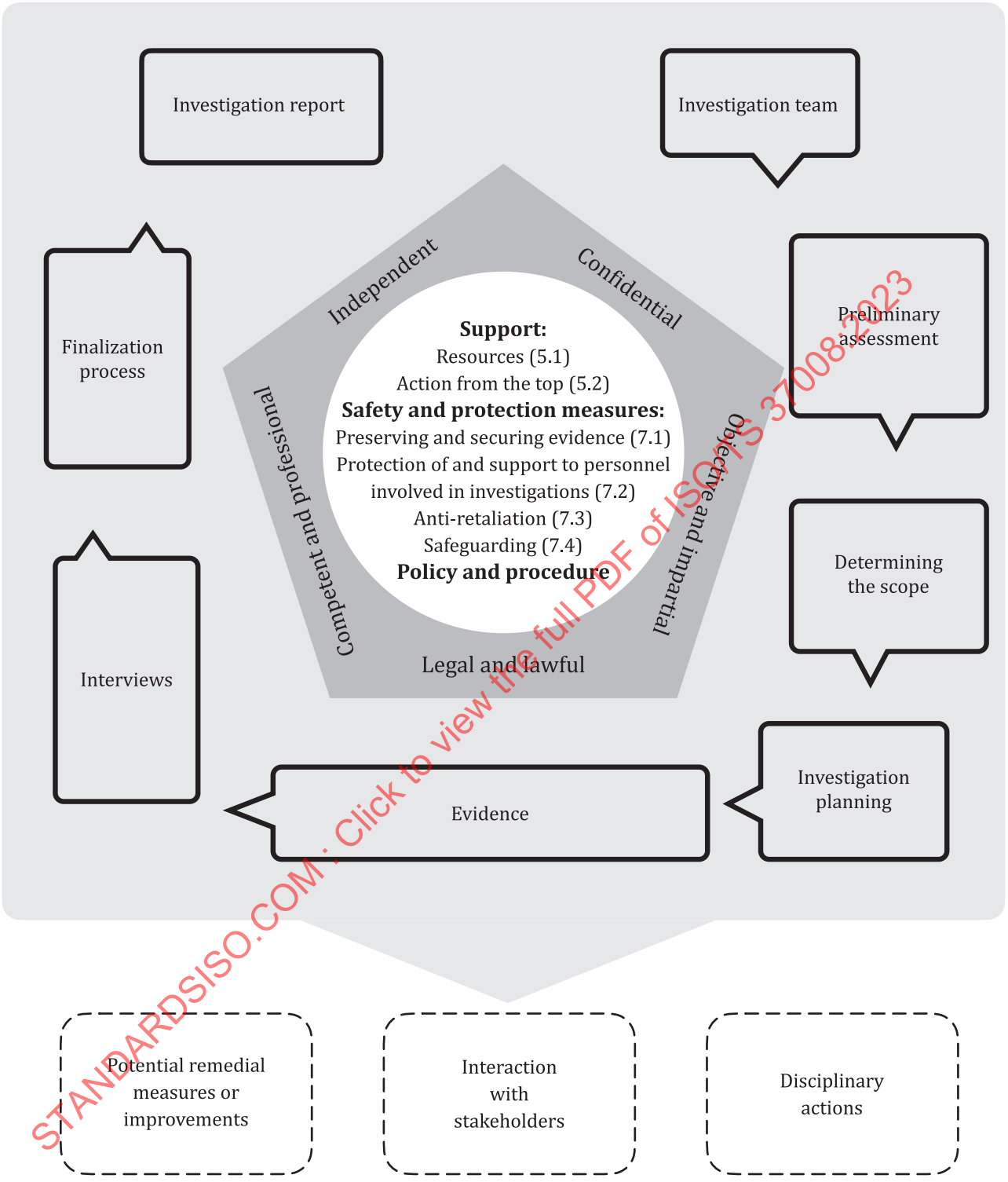

Figure 1 — Overview of the investigative process

Internal investigations of organizations — Guidance

1 Scope

This document gives guidance on internal investigations within organizations, including:

— the principles;

— support for investigations;

— establishment of the policy, procedures, processes and standards for carrying out and reporting on an investigation;

— the reporting of investigation results;

— the application of remedial measures.

This document is applicable to all organizations regardless of type, size, location, structure or purpose.

NOTE See Annex A for guidance on the use of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 37001, *Anti-bribery management systems — Requirements with guidance for use*

ISO 37002, *Whistleblowing management systems — Guidelines*

ISO 37301, *Compliance management systems — Requirements with guidance for use*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 37001, ISO 37002, ISO 37301 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
internal investigation
professional fact-finding process, initiated by or for an *organization* (3.3), to establish facts in relation to alleged or suspected wrongdoing, misconduct or noncompliance

3.2
risk
effect of uncertainty on objectives

[SOURCE: ISO 31000:2018, 3.1, modified — Notes to entry deleted.]

3.3
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 37301:2021, 3.1, modified — Note 2 to entry deleted.]

3.4
need to know
legitimate requirement to know or have access to a minimum amount of sensitive information

[SOURCE: ISO 19650-5:2020, 3.4, modified — "of a prospective recipient of information" deleted, "or have access to" replaced "to access, or to possess", and "a minimum amount of" added to the definition.]

3.5
investigator
person(s) appointed to manage or carry out an investigation

3.6
lead investigator
person leading an investigation

3.7
stakeholder
person or *organization* (3.3) that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO 37301:2021, 3.2, modified — "interested party" deleted as the preferred term.]

3.8
internal investigation function
person(s) with the organizational responsibility for investigations

3.9
compliance function
person or group of persons with responsibility and authority for the operation of the compliance management system

[SOURCE: ISO 37301:2021, 3.23, modified — Note 1 to entry deleted.]

3.10
governing body
person or group of persons that has the ultimate responsibility and authority for an *organization's* (3.3) activities, governance and policies and to which *top management* (3.11) reports and by which top management is held accountable

[SOURCE: ISO 37301:2021, 3.21, modified — Notes to entry deleted.]

3.11
top management
person or group of people who directs and controls an *organization* (3.3) at the highest level

[SOURCE: ISO 37301:2021, 3.3, modified — Notes to entry deleted.]

4 Principles

4.1 Independent

An internal investigation should not be influenced or controlled by other people, events or incentives in relation to the subject matter that is being investigated.

NOTE See A.3.1 for guidance.

4.2 Confidential

All documents and information gathered in the context of an investigation, including records, evidence and reports, should be treated in a confidential and sensitive manner. The documents and information should only be revealed on a "need to know" basis and investigators should be aware of applicable statutory laws and regulatory requirements.

4.3 Competent and professional

An internal investigation should be conducted by investigators who have professional skills, knowledge, experience, attitude and capacity to ensure the quality of their work.

An internal investigation should be conducted with integrity, fairness, truthfulness, tenacity, trust, emotional intelligence, good judgement and diligence, and completed in a timely manner.

NOTE See A.3.2 for guidance.

4.4 Objective and impartial

An internal investigation should be free from conflict of interest, conducted objectively and based on factual evidence. The investigation should not be influenced by personal feelings, interpretations or prejudice.

NOTE See A.3.3 for guidance.

4.5 Legal and lawful

Those establishing or conducting an internal investigation should identify the regulations and applicable statutes and legislation in all applicable jurisdictions to ensure the legality of the investigation.

NOTE See A.3.4 for guidance.

5 Support for internal investigations

5.1 Resources

The governing body should support the establishment, implementation, maintenance and continual improvement of internal investigations, for which top management of the organization should provide adequate resources.

Resources can include but are not limited to personnel, financial, technical and organizational infrastructure. These resources can be provided internally or externally.

NOTE See A.4.1 for more information.

5.2 Leadership and commitment

The governing body, top management and others in the appropriate positions should demonstrate leadership and commitment to an independent, objective, impartial and confidential internal investigation.

The governing body, top management and others in the appropriate positions should be reasonably informed, according to the agreed communication plan, the internal guidelines and policies preset, or as investigators deem necessary.

NOTE See A.4.2 for guidance.

6 Establishment of investigation policy or procedure

The organization should establish and implement an investigation policy or procedures that:

— define the investigation scope, process, responsibilities and capabilities of internal investigators;

— make a clear link to the organization's "whistleblower" or "speak up" procedures;

— require timely and appropriate action every time when a concern is raised;

— ensure the investigation is carried out with respect to the rights of the persons involved;

— empower and enable investigators to carry out investigation work;

— require cooperation in the investigation by all personnel;

— ensure the investigation is carried out by, and reported to, the personnel who are independent of the investigation;

— require the output of the investigation, including any limitation, challenge or any other concern of the investigation, to be appropriately documented, reviewed and reported;

— require that investigation is carried out confidentially and information is only shared with people who need to know;

— require that the organization should have policies or processes in place to stop unlawful actions immediately, also during an ongoing investigation;

— require that lessons learned or recommendations arising from investigations are used to prevent the recurrence of wrongdoing;

— require that the policies and procedures are regularly updated with learning from internal investigations.

NOTE See Clause A.5 for guidance.

7 Safety and protection measures

7.1 Preserving and securing evidence

From the beginning of the process, investigators should start to identify where relevant evidence can be stored.

An investigator should work with the relevant functions in the organization to establish whether any key witness or investigated personnel are already in the process of leaving the organization, for whatever reason.

The organization should have policies or processes to prevent anyone from tampering with witnesses and from intentionally or unintentionally deleting, destroying, altering, transferring or concealing

any form of information, data or records, which can be used as evidence, and subject the person to disciplinary measures as a breach of code of conduct.

The organization should also set protective measures to prevent information acquired in the course of the investigation from being given to persons without a need to know.

NOTE See A.6.1 for guidance.

7.2 Protection of and support to personnel involved in investigations

The organization should take measures to ensure that:

— all investigation activities, including interviews, are carried out in the absence of any form of threat, promise, inducement or oppression;

— inquiries and interviews are conducted in a discreet manner and reasonable level of privacy;

— the evidence given by the witnesses is kept confidential.

NOTE See A.6.2 for guidance.

7.3 Anti-retaliation

The organization should adopt measures to ensure that witnesses, whistleblowers, investigators, interviewees, subjects of investigation, and the personnel taking decisions on remedial measures and disciplinary actions have protection from any form of pressure, intimidation, threat, harassment and any other harmful conducts.

NOTE See A.6.3 for guidance.

7.4 Safeguarding

The organization should protect the physical and psychological well-being of anyone participating in the investigation.

8 Investigative process

8.1 Investigation team

8.1.1 Appointment of the investigation team

Top management or the governing body should appoint or authorize a person or team to conduct an investigation unless an existing investigation charter pre-sets the process of the appointment. In case the current management has a conflict of interest, the management of the next level should make such an appointment or authorization. An investigation can be assigned to external investigators.

NOTE See A.7.1 for more information.

8.1.2 Investigation reporting line

The governing body, top management or other people in the appropriate position according to the organization's internal policies should appoint an investigation reporting line who will be responsible for applying sanctions and recommending further follow up actions to the investigation.

The investigation team should keep the investigation reporting line including roles, responsibilities and authorities updated regularly or at defined intervals, and submit the investigation report for review.

The responsibilities of the investigation reporting line include but are not limited to:

— assessment of the nature of the allegation(s);

— checking any possible conflict of interest;

— reviewing the possibility of future interactions with authorities and other stakeholders regarding the investigation results;

— consideration of the severity or the seriousness of the issue;

— assessment of the potential financial, reputational or regulatory risk to the organization.

8.2 Preliminary assessment

The investigation team should conduct a preliminary assessment of the allegation.

The investigation team should consider the seriousness and credibility of the allegation presented and whether the allegations are sufficiently specific to start an investigation.

Where possible, the investigation team should consider reaching out to the whistleblower and ask for additional details in relation to the allegations, then evaluate whether a full-scale investigation is needed and use the assessment results to plan the investigation.

The results from the preliminary assessment should be documented clearly. In cases where further investigations are required, it should be reflected by a documented decision.

NOTE See A.7.2 for more information.

8.3 Determining the scope of the investigation

8.3.1 Scope

The investigation team should consider the outputs of the preliminary assessment, if any, to determine the scope of the investigation so that the investigation can be conducted effectively and adequately.

Before determining the scope of the investigation, it is important to establish the intended objective(s) of the investigation, such as:

— whether the investigator is required to simply discover the facts of a particular incident;

— whether the investigator is required to make a determination regarding whether there is any breach of organizational policy or a potential violation of law;

— whether the investigator has to make a recommendation regarding what action should be taken in case a breach is identified.

8.3.2 Scope changes

If as part of the investigation, the investigation team becomes aware of additional violations of law, organizational policies or criminal activities, then the investigation scope should be adapted accordingly. The change in scope should be documented.

8.3.3 Determination elements

When determining the scope of the investigation, the investigation team should consider critical elements, which include but are not limited to:

— substance: the specific allegation(s);

— interval: the period of time that the investigation should examine;

— geography: which region(s) or country(s) will be covered by the investigation;

— location: where any specific alleged incident(s) took place;

— persons: who allegedly conducted a breach.

8.4 Investigation planning

The investigation team should set out an investigation plan. The plan should outline the following factors:

— the background information, scope, timeline, purpose and objective of the investigation;

— the personnel required to be interviewed or to provide information to assist the investigation;

— internal or external resources required and available to achieve the objective and whether expert resources are needed, such as forensic accountants, external counsels, external investigators, industry experts or digital forensics experts;

— an evaluation of whether any employee's or custodian's labour contract must be suspended for the duration of the investigations and physical access to offices or IT systems revoked;

— potential sources of evidence and how to deal with evidence preservation, collection and review;

— how to conduct interviews, including the interview and notification schedule;

— whether any person subject to the investigation needs or requires legal representation, if permissible, and/or a support person to accompany during the interview;

— whether there is any significant legal issue;

— the risks and/or challenges the subject matter of the investigation can cause to the investigation and to the organization, and what strategies are to be used to mitigate or eliminate them;

— how the investigation should be recorded and which stakeholders should be reported to, when and in what level of detail;

— whether the organization is required to make a self-disclosure to the concerned government authority in line with the reporting requirements.

The investigation plan should be treated as a live document and should be updated as the situation changes to ensure an investigation meets the scope, objective and fundamental principles. Changes to the investigation plan should be documented.

NOTE See A.7.3 for guidance.

8.5 Maintaining confidentiality

The flow of information should be controlled on a need to know basis and kept confidential during the whole investigation process.

When necessary, the lead investigator may brief the relevant stakeholders identified in the investigation plan.

NOTE See A.7.4 for more information.

8.6 Liability caution to deter disclosure

8.6.1 Written caution notice

A written caution notice is recommended to be issued to the stakeholders to highlight the significance of the requirement to maintain confidentiality, the negative impacts of disclosure (accidental or otherwise) and the possible liabilities for disclosure.

Negative impacts of the disclosure include but are not limited to tampering with or deleting evidence, causing harm to persons involved in the investigation or causing damages to the organization. A breach of confidentiality may lead to sanctions and liability for the individuals who cause the breach.

NOTE See A.7.5 for guidance.

8.6.2 Verbal caution notice

Under certain circumstances, a verbal caution notice can be more appropriate than a written caution notice to the stakeholders. It should be decided by the lead investigator when and how it should be communicated. A verbal caution notice should include the main aspects as stated in the written caution notice. The lead investigator should keep a record of any verbal cautions issued, and may inform the stakeholders of this record.

The caution should include advising the person not to do anything that can interfere with the investigation process or impede the fact gathering.

8.7 No interference

The organization should take measures to avoid or stop interference in the investigation. This can include interference from external parties, other organizations and inside parties such as certain management or other departments. The lead investigator should report any relevant attempt to interfere in the investigation to the investigation reporting line or to the management of the organization according to the investigation policy or procedure, or in the way that the lead investigator deems appropriate.

8.8 Evidence

8.8.1 Document collection and review

The investigation team should take all the control measures to safely obtain, secure, organize and review all necessary documents collected from internal or external parties.

Investigative activity should consider the examination of all applicable evidence.

The main purpose of reviewing these records is to spot critical documents essential to the investigation. As for reviewing on a large scale, using technological or digital tools or engaging outside service providers or counsels can be considered.

NOTE See A.7.6.1 for guidance.

8.8.2 Electronic data collection, preservation, analysis and review

The investigation team should work with the information technology department or a third-party service provider when the analysis of any electronic evidence is required in order to identify, preserve and analyse electronic data. There are technology platforms and search/e-Discovery tools which can aid the review of digital data and manage digital data review workflow. Investigators should consider the use of technology and subject matter experts to aid the retrieval and review of electronic data.

The investigation team and the information technology department or third-party service provider should implement proper measures to secure all captured electronic data.

Personnel conducting electronic data collection, analysis and review should have the generic competence described in ISO/IEC 27037:2012.

NOTE See A.7.6.2 for guidance.

8.9 Interviews

8.9.1 Preparations

Before conducting the interview(s), an investigation team should do the following:

— Draft an initial list of the individuals to be interviewed.

— Prepare an interview plan including an outline of topic areas, questions if deemed necessary, and documents, emails or other materials to be used during the interview, and also decide a schedule for the timing and sequencing of interviews. Interviews should be scheduled in a manner to prevent interviewees from tampering with interviewing questions and answers. The interview plan should consider the roles of interviewers and the potential responses from the interviewee.

— Adopt appropriate interview techniques.

— Conduct interviews using appropriate techniques in which the interviewers should have sufficient competence.

— Assess the local culture and ecosystem prior to determining the team composition for an interview.

NOTE 1 In certain geographies, it can be recommended that if the discussion is with a female, it would be appropriate for the investigation team to include a female in the room for discussion.

— Review and compile relevant documents, as applicable.

— Take measures to conduct the interviews in an environment that is free of outside interference and disturbance and which can ensure confidentiality.

NOTE 2 See A.7.7.1 for guidance.

8.9.2 Conducting an interview

Steps should be taken to ensure that an interview, particularly with a subject of an investigation, is witnessed where appropriate. This can involve having two interviewers or an interviewer and a note-taker, or otherwise recording the interview, where appropriate and permissible. Care should be taken to ensure that there is a proportionate number of interviewers present to avoid being oppressive. The interviewers should consider the language in which the interview will be conducted. Arrangement should be made for translation if the interviewers do not speak the language understood by the interviewee.

The interviewer should, as a method for fact-finding, clarify with the interviewee any incoherent or conflicting information.

Upon conclusion of the interview, the interviewer should seek acknowledgement from the interviewee that the statement documented is true and accurate to the best of their knowledge and ask if they have anything further to add or clarify.

An accurate record of the interview should be taken. Interviewers should follow policies and procedures for recording interviews and take local law into consideration. Interviewees may sign a record of interview where this is appropriate and permitted.

While conducting the interview, the interviewer(s) should:

— pay attention to the interactions with the interviewee;

— be professional and respectful to the interviewee;

— exercise good listening skills;

— provide accurate and correct information.

NOTE See A.7.7.2 for guidance.

8.9.3 Keeping records of an interview

An interview should be adequately and appropriately documented, and the outputs should be securely stored and maintained confidential. Each documented interview may be communicated in written form to the interviewee(s). Interview records should be retained in line with the organization's data/records retention policy.

NOTE See A.7.7.3 for guidance.

8.10 Finalization process

An investigation should not be considered substantially complete unless it achieves the following:

— the investigation team is ready to make evidence-supported findings, and these findings are enough for the governing body and/or management to make a decision regarding the noncompliance incident;

— the investigation team is able to fully account for its work product to their constituencies;

— the investigation result provides a sufficient basis to initiate remedial and corrective actions.

NOTE See A.7.8 for guidance.

8.11 Investigation report

The investigation results should be recorded in writing. For investigations where litigation is contemplated and/or whether disclosure is needed to regulators (e.g. regulated sector), legal advice should be obtained on the (confidential) treatment of investigation reports and documents. Investigation records (which include records of interviews) and final investigation reports should be factually and accurately communicated.

The investigation team should gather and record the working papers to support the report.

The investigation report should be made in accordance with the documentary, audio, visual and oral evidence.

The investigation report should contain a full explanation of the relevant facts, limitations and constraints encountered and be limited to the scope of the investigation.

The investigation team should be aware of all applicable laws and follow the organization's retention policy in relation to preservation of all records and results. The investigation team should ensure the security of the data so that it is not misused for other purposes and it is adequately protected (e.g. from loss of confidentiality, improper use or loss of integrity).

NOTE See A.7.9 for guidance.

9 Potential remedial measures or improvements

9.1 Proposal of remedial measures and improvements

The investigation team may, subject to the organization's requirements, propose appropriate remedial measures to be implemented based on the results of the investigation to minimize the impact of violations and improve internal controls of the organization's compliance programme. Root cause

analysis methods should be used to arrive at the most appropriate remedial measures and improvements to ensure that the root causes are being appropriately, sufficiently and effectively addressed.

9.2 Interim remedial measures

As the investigation progresses, the investigation team may highlight compliance gaps, violations of law and make recommendations to the governing body, top management or the compliance function to take urgent remedial measures.

The investigation team should report to the compliance function if requested, to assist in developing a provisional plan on interim measures. The plan should state clearly the compliance gaps or vulnerabilities and the goal(s) these measures intend to reach.

9.3 A final plan for post-investigation remedial measures

The organization's function assigned according to the correspondent policies or procedures should design a final remediation plan based on the investigation report.

The post-investigation remedial measures should be broken down to specific steps with corresponding tasks assigned to a responsible person for adequate and timely implementation.

A thorough assessment of the plan should be carried out by the compliance function to ensure effectiveness and practicality.

9.4 Proportionality of remediation and improvement measures

In formulating the final remediation plan, the organization's function assigned according to the correspondent policies or procedures should consider the seriousness of the breaches revealed by the findings of the investigation report. It should then consider whether to adjust the existing organization's compliance programme by creating new or modifying existing policies or procedures, strengthening or modifying compliance monitoring or providing additional compliance training.

9.5 Monitoring and enforcement of remedial measures

The implementation of the remedial measures should be monitored and enforced for their effectiveness by the appropriate function within the organization or externally appointed.

The organization should revisit the compliance programme to determine whether it needs to be reviewed and adjusted in light of the remediation plan.

NOTE See Clause A.8 for guidance.

10 Interaction with stakeholders

10.1 General

The organization and the investigation team should have effective communication channels with stakeholders.

10.2 Planning

The organization should identify relevant stakeholders for communication. Communication with these stakeholders should be carried out through the investigation team or directly through other relevant function (e.g. management, compliance functions, human resources, public relations) as appropriate.

Each interaction should be done purposefully with pre-planned messages and scripts and in alignment with the inputs of the investigation team and of the organizational functions that have expertise and interest in the correspondent interaction.

10.3 Measures for the communication process

In communicating the investigation findings, the organization should seek input from the investigation team.

10.4 Effective communication channels

The investigation team should make plans for effective communications with all relevant stakeholders to ensure that the daily operations of the organization and the investigation can both continue.

The communication plan should aim at addressing important questions and minimizing any negative impact on operations. The organization should make a determination of what level of information the different stakeholders have the right to know.

The compliance function should decide on accompanying measures contingent on the outcome of a given interaction in order to carry out the investigation as matters progress. Typical measures include pre-emptive disciplinary actions, disclosures to government authorities, business alterations, etc. These measures should be assessed professionally by the organization before being taken. Before deciding on the measures, the organization should consult with the appropriate departments within the organization on the measures that concern them.

10.5 Government and regulator communication

The investigation team should plan to communicate with government authorities and regulators on the specific issues under investigation, if applicable. Before communicating with them, the organization should consult its internal or external legal advisers and relevant guidelines to make sure the interests and rights of the organization are fully protected.

10.6 Self-disclosure to the authorities

On the basis of the investigation progress, the investigation team should provide the necessary evidence or information to the organization's legal and compliance function to advise the organization's governing body or top management to evaluate whether the organization should make a self-disclosure to the authorities, e.g. for liability reduction or exoneration. Decision-makers should consider self-disclosure guidelines provided by the relevant regulatory or government authority and the possible legal consequences of self-reporting. For the assessment of legal consequences, the organization should consider seeking professional legal advice.

NOTE See Clause A.9 for guidance.

11 Disciplinary actions

On the basis of the final report, disciplinary actions against the concerned personnel or organizations can be taken.

NOTE See Clause A.10 for guidance.

Annex A
(informative)

Guidance on the use of this document

A.1 Background and scope

A.1.1 General

The guidance in this annex is illustrative only. Its purpose is to indicate in some specific areas the type of actions that an organization can take in managing and conducting investigations. It is not intended to be comprehensive or prescriptive.

A.1.2 Scope

Government law enforcement actions often bring about the need to manage and conduct an investigation as a part of a fact-finding effort and then decide which remedial measures should be taken. These enforcement actions can relate to issues such as export controls, sanction compliance, money laundering, antitrust, bribery, fraud and anti-corruption issues.

Civil actions and whistleblower incidents can be reasons for internal investigations as well so that the concerned organizations can find out what triggered the actions and incidents and then implement appropriate measures to reduce liabilities and prevent reoccurrence.

A.2 Normative references

The normative references relate to the terms and definitions that apply for this document. Users can refer to them and to the Bibliography for other information and International Standards that are relevant to internal investigations.

A.3 Principles

A.3.1 Independent

An internal investigation should be a systematic, independent and documented process for identified facts and objective evaluation, with the expectation to determine whether and to what extent any wrongdoing has occurred, is occurring or is likely to occur. To make sure of the principle of independence, objectivity and impartiality of investigation, the investigation team should act without personal preference and with no connection or relationship with the person subject to an investigation, the whistleblower and other interested parties. There should be well-documented job descriptions, authority and any form of self-declaration to investigation functions and to avoid potential conflicts of interest and bias.

The investigator should have the authority to conduct the investigation, and may recommend appropriate corrective or remedial actions, and to facilitate decision-making. The investigation should not be treated as a reprisal against the whistleblower, witness and interested parties but as a fact-finding process.

A.3.2 Competent and professional

An investigator should have general knowledge and skills or have undergone specific training and instruction to conduct an investigation. The investigator should have acquired knowledge and skills in investigation principles, processes and methodologies. The investigator should be able to:

— prepare, conduct, report and close an investigation;

— understand the types of risks and opportunities associated with the business operation of the organization;

— verify and confirm the relevance and accuracy of the collected information;

— relate to applicable statutory laws and regulatory requirements.

The evidence of knowledge and skills can be demonstrated by the job or project experience, certificates, educational background and training, including continuous professional development (CPD) and continuous professional education (CPE).

An investigator should act professionally, respecting and following the principles, code of conduct, policies and procedures of the organization. The investigator should exhibit credibility and trustworthiness by being consistent in an investigation.

The investigator should demonstrate his or her sense of responsibility during the investigation by being polite and caring.

A.3.3 Objective and impartial

An investigator should not promise anonymity or anything else in exchange for cooperation. The person subject to an investigation should be notified of any organizational policy that requires his or her participation, but the investigator should not offer any assessment of legal liability, any description of applicable "whistleblower" protections or anything else resembling legal advice. The investigation team should not initiate any action which can be detrimental to the objectives of the management or against the policies of the organization.

If the person subject to an investigation requests legal representation, the organization should be aware of all applicable laws and practices and should not obstruct or unfairly disadvantage the person making the request.

If applicable, an investigator of an organization should notify the person subject to the investigation that the investigator represents the organization rather than the person under the investigation. The attorney-client privilege (if applicable) belongs to the organization, not the subject person. The organization may waive the legal privilege at its own discretion, if permitted.

A.3.4 Legal and lawful

An investigation should be conducted in awareness of laws and regulations. The decision to conduct an investigation is by itself not an accusation without any presumption of guilt and is to be treated as a neutral fact-finding process.

The subject(s) identified as the alleged wrongdoer in the investigation should be informed of having a duty to cooperate with the investigator, as long as such cooperation does not merely require them to admit guilt. The subject(s) should be given the right to respond as required and the option to be assisted. The subject(s) should not interfere with the investigation. Evidence should not be withheld, destroyed or tampered with, and all parties involved in internal investigation should not be influenced, coached, threatened or intimidated.

Before, during and after the investigation, there should not be any harassment, restriction of movement or violation of privacy against any parties involved in internal investigation.

The outcome of the investigation can lead to the conclusion of the investigative report that an improper or unethical action or non-action has not been committed, as the case can be.

A.4 Support for internal investigations

A.4.1 Resources

Resources may include but are not limited to personnel, financial allocation and other organizational functions such as internal audit, information technology, security solutions, legal expertise, professional development and training, and the compliance function. These resources can be provided internally or externally. Further description of the resources mentioned above is as follows:

— Personnel (human resources): sufficient and competent personnel to apply sufficient time to their relevant function responsibilities so that the internal investigation can function effectively. This includes assigning sufficient human resources (either internal or external) to the investigation.

— Financial allocation (financial resources): sufficient budget is made available, including for the internal investigation function, so that the internal investigation can function effectively.

— Organizational function (physical resources): necessary physical resources are made available, including for the internal investigation function, so that the internal investigation can function effectively.

The resources can be outsourced to lawyers, external auditors, digital forensic and forensic accounting experts, investigators, communication experts and others when necessary.

A.4.2 Leadership and commitment

The governing body and top management of the organization should ensure that the internal investigation is carried out in an independent, objective, impartial, accountable and confidential manner without any interference from the top-level management.

There should be cooperation among the management, the investigation team, the whistleblower(s), witness(es), subject(s) and other interested parties, and support should be provided whenever there is a need and where it is deemed necessary to assist in the investigation.

No person should be left unheard, and the implicated subject always has the right to the benefit of the rules of natural justice so as to be informed of the specific allegations, to be heard and to defend himself or herself before any disciplinary action is taken. Similarly, there should not be any selective enforcement of investigation policies.

Protection and support should be accorded even if the investigation reveals that the whistleblowing is inadvertently mistaken or the allegation is not substantiated.

A.5 Establishment of investigation policy or procedure

This document provides guidance on how the organization should establish an investigation policy and procedure which takes into consideration various factors, including applicable laws, legal obligations, the context of business, size of an organization, investigation processes, reporting structure, protection of parties that raise concerns and potential liabilities the organization can face. Internal investigations can directly or indirectly cause legal risks if not properly managed.

Legal opinion should be sought where there are legal implications. This is especially so when sensitive or privileged information is identified in the course of the investigation. Legal opinion should also be sought on whether there is a regulatory or statutory obligation to report certain criminal offences (including potential or actual financial loss to the extent quantified) that is identified in the course of the investigation. All investigations should be conducted with the assumption that the case will end up in a court proceeding, and thus investigation procedures should be able to stand up to the scrutiny of the court.

A.6 Safety and protection measures

A.6.1 Preserving and securing evidence

There should be reasonable measures to prevent the deliberate or unintentional deleting, destroying, altering, transferring or concealing of any of the evidence (which includes physical, digital or testimonial evidence) or information useful to the investigation. Witnesses' testimonies are also an important kind of evidence. The organization may put internal policies in processes, such as banning resignations of employees under investigation and compelling all relevant personnel to provide and protect evidential information. One of the ways to preserve evidence can be imposing a minimum retention period for company laptops used by pre-identified personnel of sensitive positions after the personnel leave the organization. Such laptops, will be kept under safe custody so as to preserve forensic evidence in the event investigations are commenced against these personnel.

It is also important to prevent information acquired in the course of investigation from leaking out to unauthorised persons, including the person under investigation. One option to mitigate the risk of evidence loss is to have in place a policy of securing the evidence at the earliest opportunity. It can happen that a person subject to an investigation places a wiretapping or secret recording device or an ongoing mobile phone in the office, conference room and other rooms for information collecting that is related to the investigation. Therefore, the organization should have a policy to communicate the need for confidentiality to all parties involved during the investigation (e.g. witnesses, interviewees), for example:

— provide tutorials on security aspects for employees in key positions and establish a sense of anti-wiretapping;

— control key factors such as the scope of people entering and leaving an investigative space, access control, entrance and exit monitoring, and strictly implementing the visitor registration system;

— employ specialized experts and use professional equipment to conduct regular and/or ad hoc anti-wiretapping checks of key areas;

— use anti-wiretapping bags to bag the mobile phone(s) of the subject of the investigation as well as investigators;

— place anti-wiretapping equipment in an investigative room where an investigation is held.

A.6.2 Protection of and support to personnel involved in investigations

Witnesses and investigators are important to the investigation, and therefore organizations should consider how to reasonably protect witnesses and investigators from any form of threat, promise, inducement or oppression. Providing reasonable protection of privacy on the identity of witnesses, maintaining the confidentiality of information given by witnesses and providing a comfortable and conducive environment for witnesses to provide the required information. For example, the interview should be conducted in a confidential and secured environment that is out of public view and from external interference.

A.6.3 Anti-retaliation

Witnesses and whistleblowers should also be assured of non-retaliation if concerns are raised or information provided is of goodwill and without malice. Furthermore, individuals who (or permit others to) retaliate should be subject to disciplinary action, with local law taken into consideration. The protective measures and support given to witnesses and whistleblowers will form part of the culture that the organization should seek to foster. Weak protection and support, in the long run, can result in a lack of cooperation from employees due to fear of retaliation or repercussion.

A.7 Investigative process

A.7.1 Appointment of the investigation team

An investigation team can include the following:

— professional investigator who is trained to conduct a complex case from intake to conclusion;

— security personnel who are often assigned the fieldwork, e.g. interviewing outside witnesses and obtaining public records and other documents from third parties;

— auditor who can review internal documentary evidence, schedule losses and provide assistance in technical areas of the organization's operations;

— legal counsel who can provide legal advice to the investigation, as far as the legal aspects are concerned;

— human resources personnel and legal counsel who can be consulted to ensure the law governing the rights of employees in the workplace are not violated;

— management representative who can provide any assistance;

— independent external consultant.

Reporting line(s) (direct or dotted) can be set so that the investigation result can be reported to the authorized person.

A.7.2 Preliminary assessment

Before the investigation is conducted, the investigator can perform the following non-invasive preliminary research:

— contact the complainant/informant/whistleblower;

— review all relevant overt information;

— identify the business structure present in the case;

— identify the main players;

— identify the working environment;

— identify the cultural environment;

— identify technical issues;

— identify applicable laws, regulations and rules;

— review the necessity to involve external counsel;

— review the necessity to inform litigation about aspects of the investigation.

Depending on the outcome of the preliminary research, a decision to close the investigation is made in alignment with the appropriate organizational functions.

A.7.3 Investigation planning

Investigators can refer matters for legal advice where there exists a legal professional privilege concern in the jurisdiction. Where there is no legal professional privilege consideration, but the matter has legal interest, the investigator should consider relevant case progress updates to the appropriate legal stakeholder in an agreed form.

A.7.4 Maintaining confidentiality

Anonymity aims at protecting the identity of the individuals involved in the investigation. It may be applied to the person(s) who has reported the issue (e.g. whistleblower), witnesses and/or the subject(s) of the investigation.

A code name can be assigned to the case under investigation to anonymize the investigation. A code name can also be assigned to the subject of the investigation to anonymize the subject person.

The organization may embed any relevant data privacy requirements in the investigation policies and procedures. If applicable, the stakeholders to be briefed at the start of the investigation can be the compliance or legal function and/or the person who is in charge of the relevant sector or region if this can be done without creating any conflict of interest.

A.7.5 Written caution notice

The lead investigator should email the confidentiality notice to the whistleblower or the person who provided the tip that resulted in an investigation, in addition to the persons that the lead investigator chooses to brief.

A written caution notice is recommended to be provided in relation to:

— liabilities related to breaches of confidentiality, including but not limited to admonishment, administrative penalties, termination of employment or criminal liability;

— the significance of non-disclosure, including making sure that an investigation can proceed uninterrupted.

A.7.6 Evidence

A.7.6.1 Document collection and review

A.7.6.1.1 Storing documents

Documents should be stored in a place that is secured, and where the access is restricted to the investigators only.

Electronic document access should be restricted to the relevant parties only.

See other International Standards such as ISO/IEC 27001.

A.7.6.1.2 Narrowing down of documents

If a document review is carried out on voluminous amounts of data, the investigation team should methodically reduce the number of documents under review. If necessary, investigators should develop (a string of) key terms, date range or criteria to make the process more manageable. The investigators should also consider methods to identify critical information and documents with critical information. Investigators may have to go back and forth on certain documents to refine and analyse the information.

A.7.6.1.3 Review protocol

When an investigation team starts the reviewing process, they should develop a review protocol to make the most out of the documents, flag documents as relevant to particular issues under investigation and categorize collected documents into groups for review. The review protocol can be required to be updated or edited during the course of investigation with necessary management approvals.

A.7.6.1.4 Quality control

With all potentially important documents flagged in the first round of reviewing, more senior and experienced investigators (internal or external), if necessary, may conduct a second-round review for quality control. These senior investigators should find ways to make the review more efficient by identifying irrelevant documents that can be discarded. The document reviewers should always have a technical person to consult on technical and substantive questions.

A.7.6.2 Electronic data collection, preservation, analysis and review

A.7.6.2.1 Retrieval of electronic devices

An investigator should work with the information technology department or a third-party service provider to understand and decide how electronic data are stored, retrieved and analysed, being conscious of not leaving digital footprints.

A.7.6.2.2 Planning for retrieval and analysis

Nobody but the lead investigator can decide if it is necessary to retrieve an electronic device and how to retrieve a device. The investigation team should work closely with the information technology department to retrieve the work computers, mobile phones and some other electronic devices (which contain the electronic data to review). The lead investigator should work with the information technology department to plan and carry out the retrieval process unless the information technology department is in a conflict of interest situation.

The investigation team should maintain some degree of flexibility in this process. Upon the launching of an investigation, it is necessary to retrieve the laptop of the subject person to achieve a better investigative result. In cases of emergency, the investigation team, with the help of the information technology department, should immediately retrieve the laptops, mobile phones and some other electronic devices (which contain the electronic data to review) of the subject persons.

If the data collection (i.e. forensic disk imaging of laptops, servers, mobiles, etc.) is to be conducted discreetly, the investigation team should ensure the data acquisition and management aligns with the organization's information technology policies.

A.7.6.2.3 Third-party service

A third-party digital forensic service provider can be hired to conduct forensic recovery and analysis of the data or documents retrieved from the laptops, mobile phones and some other electronic devices of the subject persons.

A.7.6.2.4 Forensic data collection

An investigation team should decide how to do forensic data analysis as follows:

— Remote data collection: if the target custodian is still employed, the investigation team may conduct a remote data collection of the custodian's work computer and consider making a full forensic image through the organization's network without the custodian's notice.

— Live data collection: where it is necessary to acquire live data from devices that are still running. Live collection of volatile data in the random access memory (RAM) can enable recovery of valuable information such as network status, decrypted application and passwords.

— Offline data collection: the investigation team may also apply offline collection to conduct full imaging using industry standard forensic tools and thorough documentation to keep the chain of custody procedures.

— Email data collection: the investigation team, with expert assistance, may collect a copy of the custodian's email data from the organization.