

ISO/~~DTS~~ 37008:202~~x~~2023(E)

~~ISO TC 309/WG 7~~

Date: 2023-~~01-16~~2023-14

ISO TC 309

Secretariat: BSI

Internal investigations of organizations — Guidance

Enquêtes internes des organisations — Recommandations

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/DTS 37008

<https://standards.iteh.ai/catalog/standards/sist/ecb27a9a-a367-4910-b034-027a5b8d3b20/iso-dts-37008>

~~DTS~~ stage

Warning for WDs and CDs

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO Copyright Office
CP 401 • CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org
Published in Switzerland.

iTeh STANDARD PREVIEW (standards.iteh.ai)

ISO/DTS 37008

<https://standards.iteh.ai/catalog/standards/sist/ecb27a9a-a367-4910-b034-027a5b8d3b20/iso-dts-37008>

Contents

Foreword	v
Introduction.....	vi
1 Scope	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Principles.....	3
4.1 Independent.....	3
4.2 Confidential.....	3
4.3 Competent and professional.....	3
4.4 Objective and impartial	3
4.5 Legal and lawful.....	3
5 Support for internal investigations.....	4
5.1 Resources.....	4
5.2 Leadership and commitment.....	4
6 Establishment of investigation policy or procedure.....	4
7 Safety and protection measures.....	5
7.1 Preserving and securing evidence	5
7.2 Protection of and support to personnel involved in investigations	5
7.3 Anti-retaliation	5
7.4 Safeguarding	5
8 Investigative process.....	6
8.1 Investigation team	6
8.1.1 Appointment of the investigation team	6
8.1.2 Investigation reporting line	6
8.2 Preliminary assessment	6
8.3 Determining the scope of the investigation.....	6
8.3.1 Scope.....	6
8.3.2 Scope changes.....	7
8.3.3 Determination elements.....	7
8.4 Investigation planning	7
8.5 Maintaining confidentiality.....	8
8.6 Liability caution to deter disclosure	8
8.6.1 Written caution notice	8
8.6.2 Verbal caution notice.....	8
8.7 No interference	8
8.8 Evidence	9
8.8.1 Document collection and review	9
8.8.2 Electronic data collection, preservation, analysis and review	9
8.9 Interviews.....	9
8.9.1 Preparations	9
8.9.2 Conducting an interview.....	10
8.9.3 Keeping records of an interview	10
8.10 Finalization process	10
8.11 Investigation report.....	11
9 Potential remedial measures or improvements	11
9.1 Proposal of remedial measures and improvements	11
9.2 Interim remedial measures.....	11
9.3 A final plan for post-investigation remedial measures.....	11

9.4	Proportionality of remediation and improvement measures	12
9.5	Monitoring and enforcement of remedial measures	12
10	Interaction with stakeholders	12
10.1	General	12
10.2	Planning	12
10.3	Measures for the communication process	12
10.4	Effective communication channels	12
10.5	Government and regulator communication	13
10.6	Self-disclosure to the authorities	13
11	Disciplinary actions	13
	Annex A (informative) Guidance on the use of this document	14
	Bibliography	26

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/DTS 37008

<https://standards.iteh.ai/catalog/standards/sist/ecb27a9a-a367-4910-b034-027a5b8d3b20/iso-dts-37008>

Foreword

ISO (the International ~~organization~~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 ~~should~~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~~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; ~~and~~
- make decisions on sanctions of management and/or employees and debarment of working with third parties involved in unethical conducts.

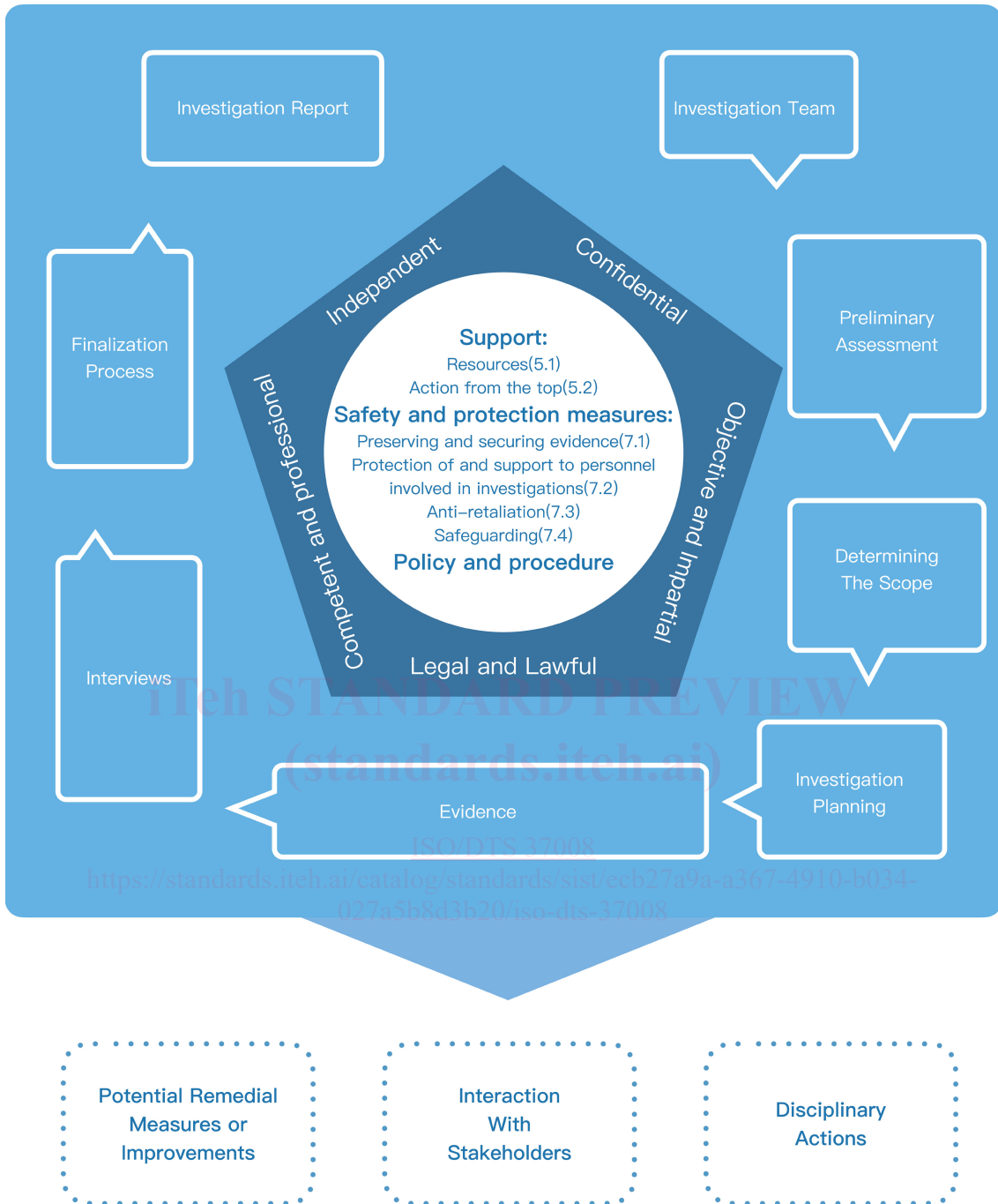
Civil actions, whistleblower reports and external investigations by regulators ~~could~~can be reasons for internal investigation as well so that the concerned organizations ~~could~~can find out what triggered the actions, reports and external investigations, then take appropriate measures.

Internal investigation is part of a compliance management system. This ~~standard~~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 ~~investigation could~~investigations can have adverse effects on an organization such as compromising the effectiveness of the compliance management system, failing to protect ~~the~~its reputation, ~~and~~ failing to detect and counter wrongdoing.

This document gives guidance for organizations to implement internal investigations based on the following principles: "independent", "confidential", "competent and professional", "objective and impartial", ~~as well as~~ and "legal and lawful". ~~It is applicable to all organizations regardless of type, size, location, structure or purpose.~~

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



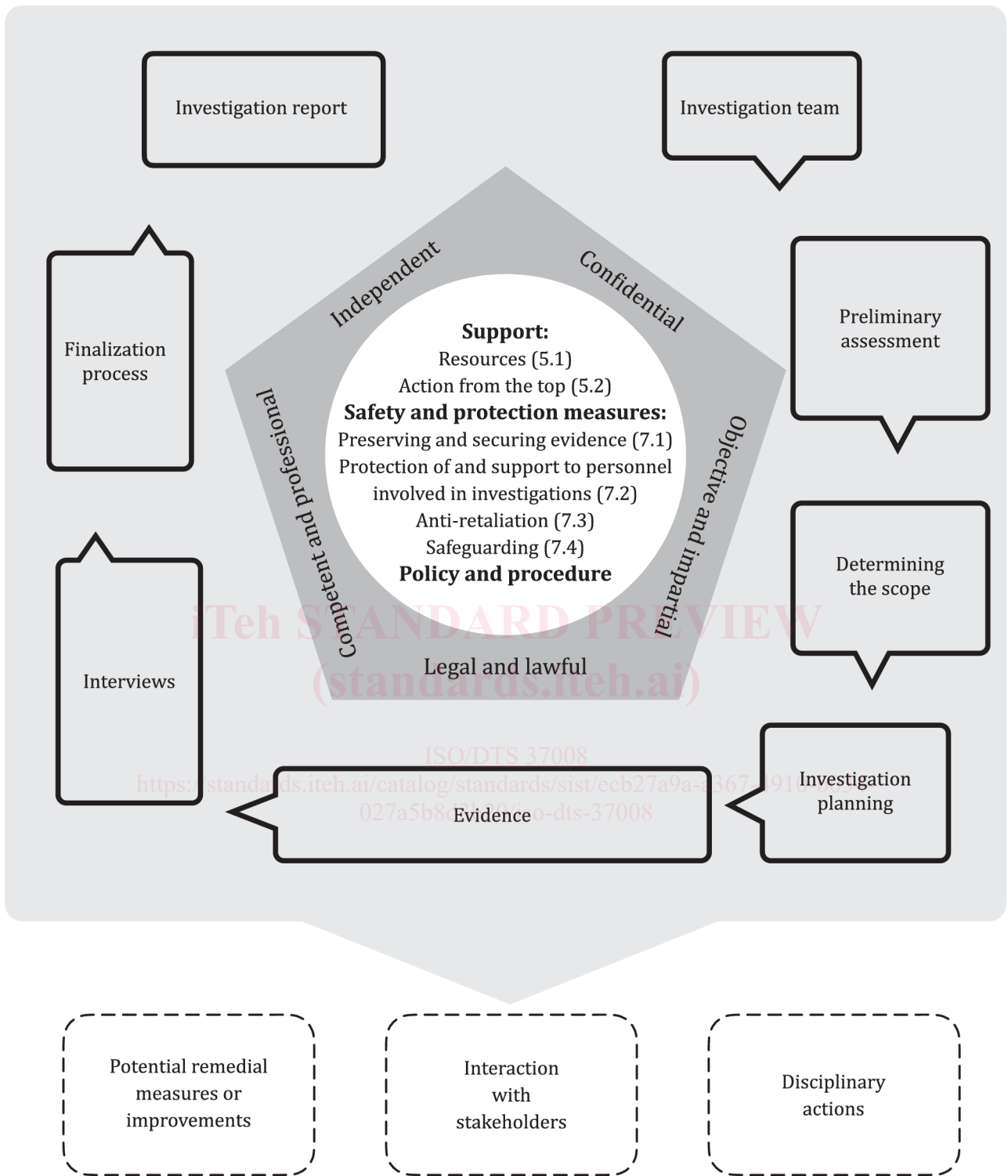


Figure 1— Overview of the investigative process

Internal investigations of organizations — Guidance

1 Scope

This document ~~provides~~~~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; ~~and~~
- the application of remedial measures.

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

NOTE See [Annex A-1](#) for guidance ~~on the use of this document~~.

2 Normative references

~~There are no normative references in this document.~~ 37008

NOTE — See [A.2](#) for guidance.

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 ~~purpose~~~~purposes~~ of this document, the terms and definitions ~~are~~ given in ISO 37001, ISO 37002, ISO 37301 and the following ~~applies~~~~apply~~.

ISO and IEC maintain ~~terminological~~~~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 ~~have been~~ 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 ~~an~~ 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 ~~has been~~ deleted.]

3.4

need to know

legitimate requirement to know or have ~~an~~ 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 — ~~The term~~ “interested party” ~~has been~~ 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, 3.2.3, modified — Note 1 to entry ~~has been~~ 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 ~~have been~~ 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 ~~have been~~ 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 ~~judgment~~ 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 [guidance](#) [more information](#).

5.2 Leadership and ~~Commitment~~ 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 and 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; ~~and~~