Managing Whistleblowing & Conduct of Investigation

The Institute of Internal Auditors

Chayce Wong

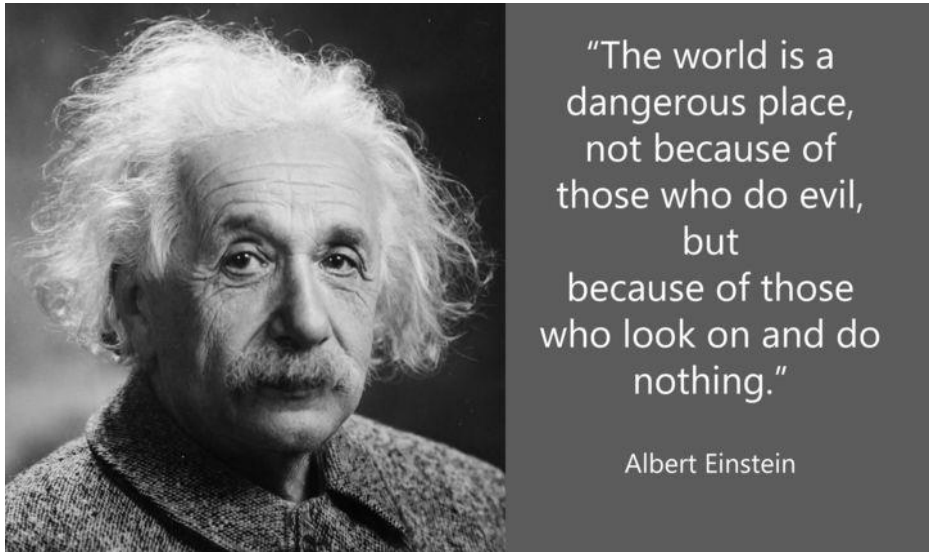
27 April 2022

IIAM Tea Talk Series

Whistleblowing

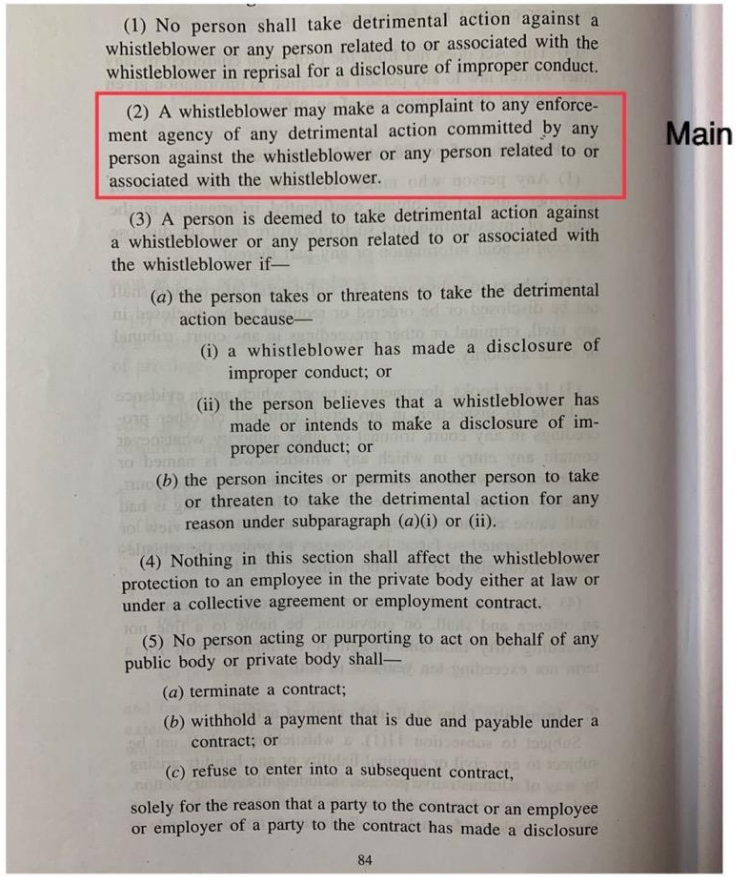
What is whistle blowing

An avenue created by laws / policy to enable people within an organization and external parties to raise concerns on the affairs of the organization without fear of retaliation, subject to the fulfillment of certain conditions.



Regulatory significance

- Whistleblower Protection Act 2010 (WPA) enacted in accordance with Malaysia's obligations under the United Nations Convention against corruption.
- Enforced on 15 December 2010.
- Serves as an external reporting system enabling employees within an organization to report any illegal or unethical practices encountered within their workplace.
- Provides whistleblowers with legal protection and protection from being penalized or dismissed by their employers.
- Disclosure must be made to an enforcement agency to 7 bodies, i.e. SPRM, the Royal Police, Securities Commission, SSM, Customs, Immigration and JPJ.



(1) No person shall take detrimental action against a whistleblower or any person related to or associated with the whistleblower in reprisal for a disclosure of improper conduct.

(2) A whistleblower may make a complaint to any enforcement agency of any detrimental action committed by any person against the whistleblower or any person related to or associated with the whistleblower.

(3) A person is deemed to take detrimental action against a whistleblower or any person related to or associated with the whistleblower if—

(*a*) the person takes or threatens to take the detrimental action because—

(i) a whistleblower has made a disclosure of improper conduct; or

(ii) the person believes that a whistleblower has made or intends to make a disclosure of improper conduct; or

(*b*) the person incites or permits another person to take or threaten to take the detrimental action for any reason under subparagraph (*a*)(i) or (ii).

(4) Nothing in this section shall affect the whistleblower protection to an employee in the private body either at law or under a collective agreement or employment contract.

(5) No person acting or purporting to act on behalf of any public body or private body shall—

(*a*) terminate a contract;

(*b*) withhold a payment that is due and payable under a contract; or

(*c*) refuse to enter into a subsequent contract,

solely for the reason that a party to the contract or an employee or employer of a party to the contract has made a disclosure

84

Main Enforcement Agency

MACC
SSM
SC
JPJ
Immigration
Custom
PDRM
BHEU
KPDNHEP

Forms of Protection

- **Protection of confidential information**
  - **Section 8 of the WPA** ~ any person who makes or receives a disclosure of improper conduct, or obtains confidential information in the course of investigation into such disclosure must not disclose such confidential information. Section 8 prohibits not only the party receiving the disclosure, but also the whistleblower making the disclosure, from disclosing confidential information.

- **Immunity from civil and criminal liability and any administrative or disciplinary action**
  - **Section 9 of the WPA** ~ a whistleblower will not be subject to any civil or criminal liability or any liability arising by way of administrative process, including disciplinary action, and any action, claim, or demand taken or made against the whistleblower, for making a disclosure of improper conduct. The inclusion of the provision, "any liability arising by way of administrative process" suggests that this protection is not limited to liability arising from legal suits but also internal actions taken by a corporation or organization against an employee, agent, or service provider that is a whistleblower.

- **Protection from detrimental action**
  - **Section 10 of the WPA** ~ protects a whistleblower and any person related to or associated with the whistleblower from detrimental action in reprisal for a disclosure of improper conduct. This protection **extends beyond the whistleblower himself**, and recognizes that the safety of these related or associated people is an important consideration for a whistleblower to blow the whistle

Circumstances For Withdrawal Of Protection

- The Whistleblower has participated in the improper conduct.
- The Whistleblower made his disclosure statements which he believed to be false or did not believe to be true.
- The disclosure of improper conduct is frivolous or vexatious.
- It involves questioning the merits of the government policy/public body.
- Made solely or substantially with the intention of avoiding dismissal or disciplinary action.
- In the course of making the disclosure of further information, commits an offence under the Act.

Limitations of Whistleblower Protection Act

- An individual is only a "whistleblower" under the WPA if he makes a disclosure of improper conduct to an **"enforcement agency",** which excludes regulatory bodies and public bodies with investigative and enforcement powers.
- Where an employee discloses improper conduct to the management of the corporation in the hopes that the management will resolve the issue, he effectively renounces any right to claim protection under the WPA. On the other hand, where an employee discloses improper conduct directly to an enforcement agency, the corporation will then have no opportunity to rectify the issues internally.
- Section 6(2)(c) of the WPA provides that disclosure of improper conduct may be made in respect of information acquired as an officer of a public body. On the other hand, government documents, data, and other information are generally classified as official secrets under the **Official Secrets Act 1972 ("OSA"), which can only be communicated with authorisation**.

  As a result, disclosing such information without authorisation — even where it relates to improper conduct — amounts to an offence under the OSA and **automatically disqualifies the whistleblower from protection** under the WPA by virtue of Section 6(1) of the WPA. Additionally, the whistleblower then faces the possibility of prosecution for an offence under the OSA which, if convicted, carries a jail term of between 1 and 7 years.

- **Section 203A of the Penal Code** makes it a criminal offence for a public servant to disclose any information or matter obtained by him in the performance of his duties or the exercise of his functions. If convicted, the public servant faces a fine of up to RM 1 million and a jail term of up to 1 year or either.

Rationale for Implementing Whistleblowing Framework

- Concerns investigated upon expeditiously.
- Combats corrupt, dishonest or improper corporate activities.
- Encourages a transparent management.
- Increases the perception of detection of misconduct is in an organization.
- Nurtures good and healthy corporate culture.
- Develops culture of openness, transparency, accountability and integrity.
- Help to ensure that problems come to light before it is too late.

The Value of "Whistleblowers"

- Whistleblowers as risk detectors
- Whistleblowers as an asset not a liability
- Establish safe internal whistleblower channels
- Corporate culture and the tone at the top
- Hire whistleblowers to utilize their expertise

What Is Not Whistleblowing?

- Questioning financing and business decisions taken by the Board
- Interpersonal grievances at work
- Complaint or grievances in terms of employment.
- Complaint over administrative issues.
- Complaint over work stress.
- Sharing with friends and families over social media.

General Malpractice

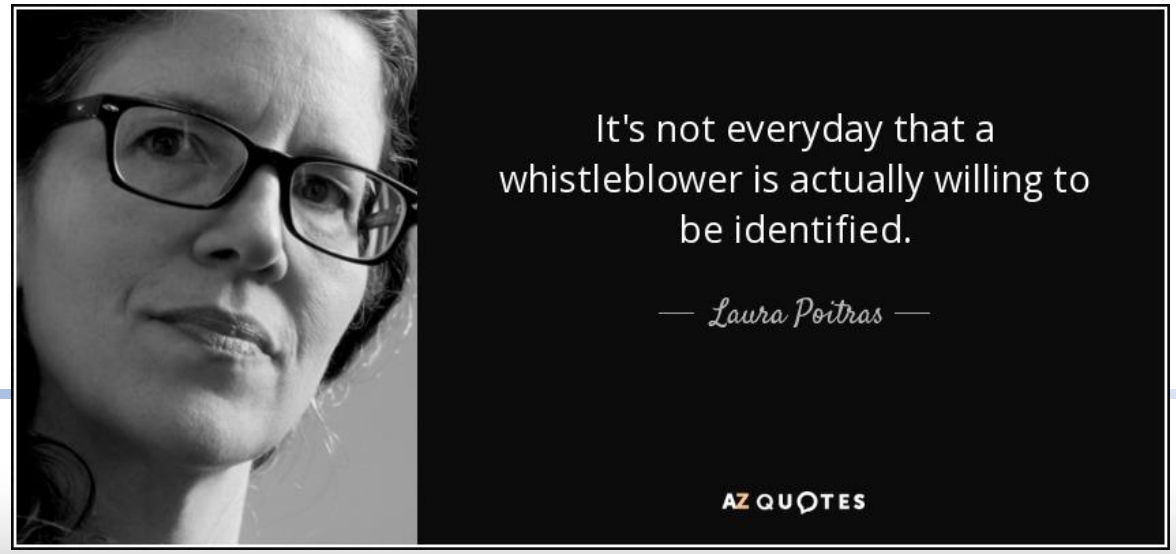
- Abuse of authority
- Breach of contract
- Negligence causing substantial and specific danger to public health and safety
- Manipulation of company data/records
- Financial irregularities, including fraud or suspected fraud or deficiencies in Internal Control and check or deliberate error in preparations of Financial Statements or Misrepresentation of financial reports
- Any unlawful act whether Criminal/ Civil
- Pilferation of confidential/propriety information
- Deliberate violation of law/regulation
- Wastage/ misappropriation of company funds/assets
- Breach of Company Code of Conduct or Policy or failure to implement or comply with any approved Company Policy
- Conflict of interest
- Bullying or harassment
- Breaches of copyright, patent and disclosure of confidential data/information to competitors/outsiders.

Factors lead to distrust in WB Process

- Lack of communication
- Inaccessibility of the hotline or WB Committee members
- Lack of transparency/ integrity of the process
- Too much emphasis on "credible" complaints
- Too many layers in WB system
- Lack of proficiency and objectivity i.e. involvement of management
- Lack of trust in the process i.e. hunting for the WB
- Inconsistent or No outcomes

Safeguards To Whistleblowers

- Confidentiality of Whistle Blower
- Protection from retaliation
- No adverse employment action



Safeguards To Whistleblowers (WBs)

- If one raises a concern under this Policy, WBs will not be at risk of suffering any form of **reprisal or retaliation**. Retaliation includes discrimination, reprisal, harassment or vengeance in any manner.
- Employee will not be at the risk of losing her/ his job or suffer loss in any other manner like transfer, demotion, refusal of promotion, or the like including any direct or indirect use of authority to obstruct the Whistle blowers' right to continue to perform his/her duties/functions including making further Protected Disclosure, as a result of reporting.
- Company will **not tolerate the harassment or victimization** of anyone raising a genuine concern.
- No action will be taken against anyone who makes an allegation in good faith, reasonably believing it to be true, even if the allegation is not subsequently confirmed by the investigation.
- Any other Employee/business associate assisting in the said investigation shall also be protected to the same extent as the Whistle blower.

Criteria for Protection

- Made in **good faith**
- **Genuine and reasonable** suspicion / belief
- **Reasonable grounds to believe truth of disclosure**
- No involvement of the Whistle blower in the subject matter of disclosure
- **Not acting for personal gain**

Anyone who abuses the procedure (for example by maliciously raising a concern knowing it to be untrue) will be subject to disciplinary action.

Avoiding retaliation

- Establish a strong pro-WB and **anti-retaliation procedures.**
- Include a **pro-WB and anti-retaliation statement** in all personal documents.
- **Audit the WB process** to ensure laws are being complied with.
- Establish and **communicate a consistent procedure** for raising concerns internally and that their concerns will be investigated fully and fairly.
- **Independence of WB and Investigation**.
- **Confidentiality and Consistency**.
- Regularly engage and train senior management, managers and supervisors. Do NOT HUNT for WBs.
- Take **stringent actions taken for retaliation**, including termination. Counsel managers and supervisors to change their mindset on WB.

The concept of no reprisal and retaliation
https://youtu.be/07wM_mRN8Fk

Avoiding retaliation

- Alert all HR personnel and senior management to the reality that the whistleblowing laws may provide discontented employees which may be costly and damaging to the company.
- **Document performance issues** as they occur. Not doing so may implicate that such problems did not exist prior to the filing of the whistleblowing concern. Documentation is crucial to prove consistency and refute claims of retaliation.
- Ensure all whistleblowing concerns are **investigated immediately** with proper planning and documentation including the outcome of the finding, including claims of retaliations, harassments and discrimination.
- Do not allow apprehension or fear of retaliation prevent you from managing or supervising employees.
- Carefully review termination or other significant negative employment actions involving employees to ensure those actions does not violate the whistleblowing policy that might provide protection to employees.

WB Channels

- Internal
  - Board of Directors
  - Independent Non-Executive Directors
  - CEO / Senior Management
  - Compliance / Integrity Officer

- External
  - Hotline

Key Success Factors - Whistleblowing

- **Provide channel** - outside the normal chain of command and can be directly routed to someone that is **independent** and has the authority to investigate and evaluate the claims.
- **Protect confidentiality**. If the investigation proceeds to the level where the employee must no longer remain anonymous, then that decision must be made carefully and with consent.
- Implement a detailed **non-retaliation policy** protecting whistleblowers who make reports in good faith.
- Reinforce a **culture of openness and transparency**. Instead of trying to limit complaints/concerns, companies should accept them and address them head on, resolving the issue to the extent possible while it remains in their control.
- Implement **records retention policy** for whistleblower reports, complaints and investigations.
- **Train senior management** on whistleblower policies, especially non-retaliation. Senior leaders can test the whistleblower hotline and share their experiences with employees, assuring them of equal treatment of complaints.
- Ongoing education/ workshops, from inclusion in a mandatory annual compliance training session to constantly displaying a poster in the company break room, is essential for getting employees to accept and embrace the idea of self-regulation using a hotline.

Conduct of Investigation

The Institute of
Internal Auditors

Why is an Investigation Necessary?

- **Provide channel** - outside the normal chain of command and can be directly routed to someone that is **independent** and has the authority to investigate and evaluate the claims.
- **Protect confidentiality**. If the investigation proceeds to the level where the employee must no longer remain anonymous, then that decision must be made carefully and with consent.
- Implement a detailed **non-retaliation policy** protecting whistleblowers who make reports in good faith.
- Reinforce a **culture of openness and transparency**. Instead of trying to limit complaints/concerns, companies should accept them and address them head on, resolving the issue to the extent possible while it remains in their control.
- Implement **records retention policy** for whistleblower reports, complaints and investigations.
- **Train senior management** on whistleblower policies, especially non-retaliation. Senior leaders can test the whistleblower hotline and share their experiences with employees, assuring them of equal treatment of complaints.
- Ongoing education/ workshops, from inclusion in a mandatory annual compliance training session to constantly displaying a poster in the company break room, is essential for getting employees to accept and embrace the idea of self-regulation using a hotline.

Investigation Process

Investigation Process

Assessment

- When assessing information that has been brought to your attention there are a number of questions that you will need to answer before taking any further action.

- If you are able to connect with the source of the information then you should ask them certain basic questions, including:
  - How do you know that this information is true?
  - When did you first know this to be true?
  - When did you last know this to be true?
  - Who else knows that this is true?

- These basic questions will establish the strength of the information, the scope of the initial investigation and assist in identifying other potential sources of information.

- In some cases, you may not be able to get additional information, and will need to rely on other information, including interviews, to answer the above questions.

Investigation Planning

Planning

- Define scope and timetable. Ensure you have agreed with stakeholders what is ‘in and out’ of the investigation remit.
- Identify the actions to be undertaken.
- Identify and brief any additional resources.
- Identify and preserve information/ material.
- Identify any legal risks (is legal support required?).
- Decide on who needs to know about the investigation and what they need to know.
- Ensure that the alleged perpetrator has the opportunity to respond to new information.

Preparing for Investigation

Planning

- Notify the Audit and Risk Committee
- Review available information and/or documentation
- Seek further information (e.g. emails, policies etc)
- Develop a set of initial questions for each witness/ interviewee
- Think about questioning technique to direct and control the interview
- Think about the people you are about to meet – what may be their state of mind?
- Try not to prejudge as this may narrow the focus and restrict the flow of information
- Inviting witnesses/ interviewee for interviews:
  - Notice or not?
  - Invite letter
  - Venue

Securing Potential Electronic Evidence

Planning

As quickly as possible, identify and secure potential electronic evidence. This might includes but not limited to:

- Computers/ laptops
- Tablets
- Electronic databases (accounting records, etc)
- Back-up tapes
- PABX system records and voice mails log
- Building access records
- Telephone recording/ Virtual meeting recordings
- Fax machines
- Mobile
- External drive/ USBs

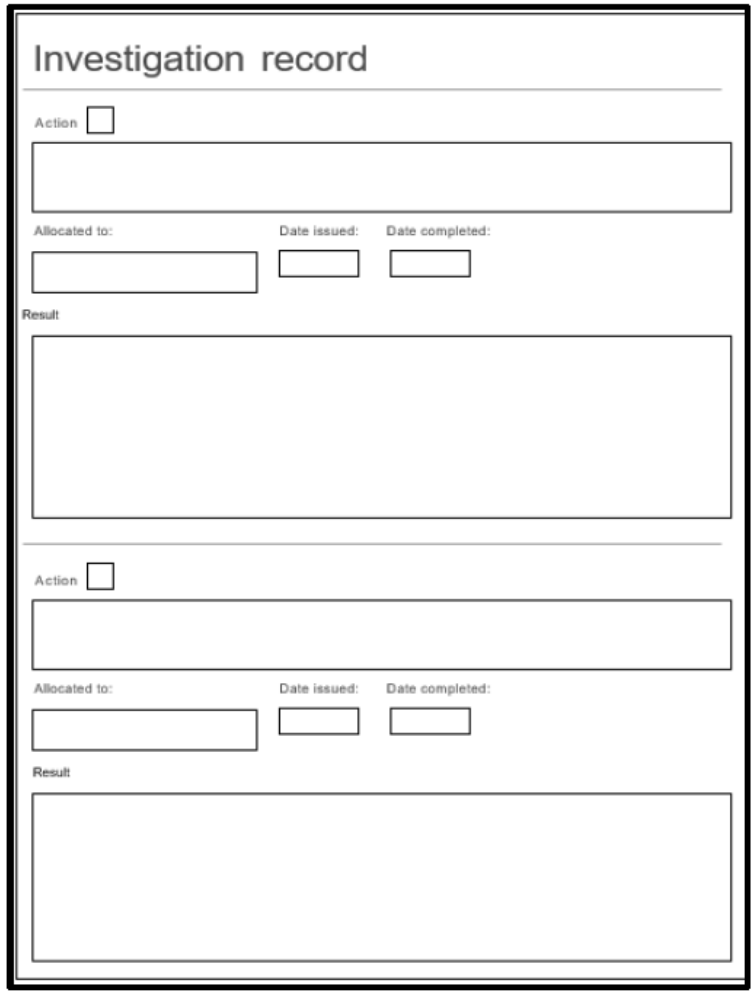
Electronic evidence is very fragile, and must be **handled with care**.

Do not let non-forensically trained staff handle / touch electronic evidence.

If there is no expertise, physically secure the devices (**keep original**)

Interview Records

Planning



Investigation record

Action ☐

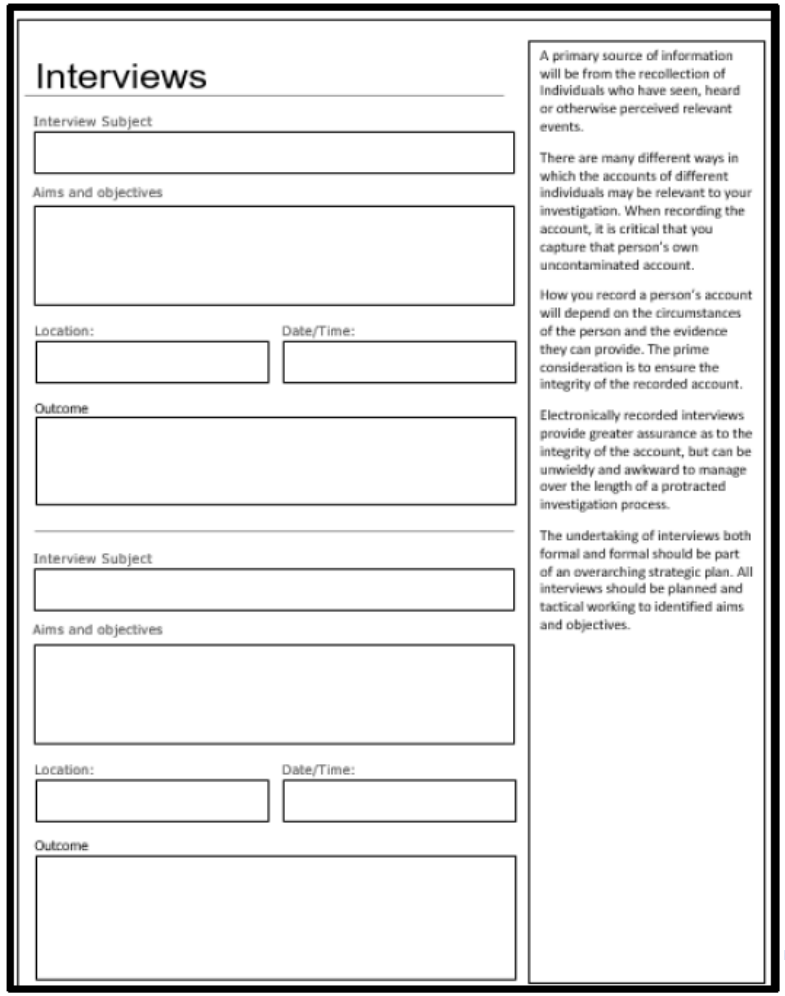
Allocated to: | Date issued: | Date completed:

Result

Action ☐

Allocated to: | Date issued: | Date completed:

Result



Interviews

Interview Subject

Aims and objectives

Location: | Date/Time:

Outcome

Interview Subject

Aims and objectives

Location: | Date/Time:

Outcome

A primary source of information will be from the recollection of individuals who have seen, heard or otherwise perceived relevant events.

There are many different ways in which the accounts of different individuals may be relevant to your investigation. When recording the account, it is critical that you capture that person's own uncontaminated account.

How you record a person's account will depend on the circumstances of the person and the evidence they can provide. The prime consideration is to ensure the integrity of the recorded account.

Electronically recorded interviews provide greater assurance as to the integrity of the account, but can be unwieldy and awkward to manage over the length of a protracted investigation process.

The undertaking of interviews both formal and formal should be part of an overarching strategic plan. All interviews should be planned and tactical working to identified aims and objectives.

Information Gathering

Implementation

Three Distinct Steps

Step 1: Collect Information

Step 2: Conduct Interviews

Step 3: Analyse Information

"Information gathering is the basic task of the investigator."

Information Gathering

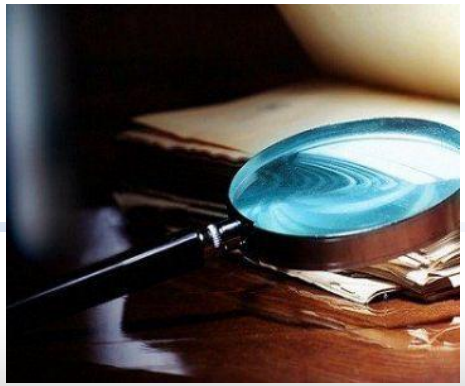
Implementation

Analysis of information gathered should enable the investigation team to compile:

- **chronology of events;**
- **summary of key documents;**
- **list of process or control gaps or weaknesses; and**
- **other data and persons involved / required to be interviewed (e. g. financial data, access control records, etc.)**

Documentary evidence should typically be reviewed before interviews are conducted.

Obtaining, Handling and Preservation of information/ documents must be conducted in compliance with strict legal requirements.



Interview vs Interrogation

Implementation

Interview

Aim to gather information and to find out the truth of what happened...

Investigative in nature

Interrogation

Aim to extract confession, incriminating statements or admissions of guilt;

Accusatorial in nature

Questioning

Implementation

Type of question	Example
Open questions	Please describe… Please tell me about… Please explain…
Confirmation questions	Who When What Where How Why
Focused questions	Elicit yes/no answers or a specific detail of information
Closed questions	Have I understood correctly? I understand you to be saying that…
Completeness questions	Is there anything else you would like to tell me before we move on?

Listening

Implementation

Ethical excuses bingo

ethicsinsight

"Everyone else does it..."	"It's for the greater good."	"I had to make a snap decision."	"I was doing it for the company,"	"That's how it's always been done."
"I'm just following orders."	"I had to hit my targets/goals."	"If I don't do it, someone else will."	"It was an important customer."	"It's just a facilitation payment - it's ok."
"I didn't think it would hurt [anyone/anything]."	"Right and wrong are relative concepts."	"The devil made me do it."	"It's a cost of doing business."	"It's how things are done in..."
"I didn't want to lose the customer."	"Our agent paid it, not us."	"I assumed it was part of my compensation package"	"Look at the bigger picture."	"I'm under so much pressure."
"Someone had to do it."	"It's a market practice."	"No one ever told me to not do it."	"I didn't know it is not allowed."	"We have been doing it for years."

Question Any Inconsistency

Implementation

- If questions don't give you an accurate view then:
  - Show me!
  - Act out!
- Feel free to ask whatever you think is relevant to the situation. The aim is to get a true picture.

Closing the Interview

Implementation

- At the end of the interview, take an adjournment to review the facts obtained in the interview.
- When the interview is reconvened, give a final opportunity to add further information and summarize the discussion.
- Emphasizes on confidentiality.

Considerations

- Review notes
- Relevant points addressed
- Confirm next steps
- Provide contact information
- Summarize facts
- Resolve inconsistencies
- Schedule follow ups
- Reiterate need for confidentiality

Written Records

Implementation

- Note your statements may be produced in court – ensure they are professional!

Interview Considerations

Implementation

- **Translation:**
  - Translators are permitted but must be independent and subject to confidentiality

- **Accompanied interviews:**
  - In general the subject of the investigation can not be accompanied

- **"Off the record" responses**:
  - There is no such thing!

- **Refusal to cooperate**:
  - Cannot force cooperation, but employees do have a duty to cooperate. Report non-cooperation in interview memorandum/report.

Analyzing Information

Implementation

From the analysis, you want to be able to:

- Establish a **chronology of events**
- Provide a clear summary of the key documents and their contents
- Identify any system or control **gaps or weaknesses**
- Confirm you have sufficient data (e.g. financial data, access control records) to confirm or refute the allegations

If the analysis indicates a gap in the information, consider:

- Requesting further information
- Carrying out additional interviews

Making Conclusion

Reporting & Closing

- **Misconduct** – An objective conclusion of facts gained including whether there has been a breach of a policy or procedure.

- **Grievance** - A conclusion about the facts obtained, determine whether there is a case to answer and provide the rationale to support this decision (e.g. Upheld / not upheld). If appropriate, put forward recommendations for the best way forward for all parties involved.

Drafting the Investigation Report

Reporting & Closing

- Ensure that the report addresses the grievance/misconduct issue alone – don't allow the scope to creep!
- Facts based
- Be specific
- Don't include/reference appendices on the grievance document – the employee does not always see the witness statements in a grievance case where it won't help resolve the situation. This might change if there is an appeal.
- Ensure any documents referenced have already been seen by the employee i.e. that there are no surprises!

Drafting the Investigation Report

Reporting & Closing

Reports should include:

- Executive Summary (in particular if the Report is lengthy)
- Summary of Allegations
- Summary of Investigation (what steps were taken and what was done during the course of the investigation)
- Summary of Factual Findings
- Outcomes, Recommendations and Conclusions

Be Specific

Keep It Short & Simple

Closing

Reporting & Closing

- Engage Line Manager of the implicated employee and HR. Present the summary report and corrective actions.
- Update the case on the Whistleblower Portal / Internal Investigation Management System (if any)
- Keep all relevant documentation collected during the investigation secured, including:
  - Report (destroy draft reports)
  - Information used in drawing conclusions
  - Relevant documents collected and analyzed
  - Interview notes
  - Handwritten notes
- Close the case in the Whistleblower Portal / Internal Investigation Management System (if any)
- Implementation of Corrective and Preventative Action is the responsibility of line management in the business. Corrective action should be consistently applied.

Investigation – Roles & Responsibilities

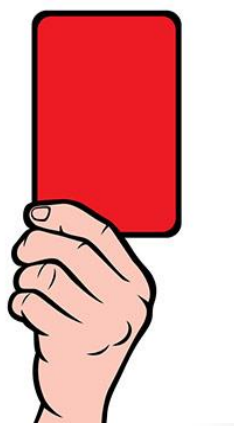
- All employees must report violations or potential violations.
- Compliance / Integrity officer:
  - Determine if a WB is an Ethical and Compliance related or grievances.
  - Respond to the complainant that their report was received and will be investigated.
  - Inform HR that there is a complaint that will be investigated and review final reports with HR and Legal Counsel
    - Align on recommendations for substantiated findings
    - If local HR is part of the allegation, then report to regional/ global HR/ Board of Directors
  - Maintain confidentiality of the reporter and witnesses
  - Investigate, document and maintain updated status in Investigation/Hotline Portal
  - Monitor implementation of any remediation actions
  - Close out the matter with the Complainant.
  - Report the WB and outcome of the investigation to Audit & Risk Committee.

Investigation – Roles & Responsibilities

- **Human Resources:**
  - Handles performance and HR related concerns.
  - Assists in interviews as needed.
  - Decides on disciplinary measures in alignment with Integrity function.
  - Assists in execution of disciplinary measures.
  - Provides input to final report to prevent future occurances of non-compliant behavior.
  - Closes out HR matters in the Hotline portal.
  - Establish anti-retaliation policies.
- **Legal:**
  - Review and approve investigative plan, as needed.
  - Assist in interviews as needed.
  - Assist when investigator needs assistance with external counsel.
  - Support Integrity Officer's review of the final investigation report and align on disciplinary actions, as needed.
- **Designated Investigator(s)**
  - Draft an investigation plan and review with Integrity Officer and Chairperson of Audit & Risk Committee prior to initiating the investigation.
  - Maintain strict confidentiality.
  - Be objective and treat witnesses and implicated person fairly and with respect throughout the investigation.
  - Prepare the investigation report outlining investigative findings, capturing the facts, interviews conducted and any relevant material to support or refute the allegations.

Misconduct / Disciplinary Process

- Having **fair, transparent and consistent process** to manage misconduct can **further strengthen employees' understanding and appreciation** of entity's Code of Conduct and policies & **boost confidence** on managing such misconduct.
- Sanction taken must be consistent with misconduct classification, no matter what level the employee is.
- All sanctions shall be documented in personal files.
- Exception must be justified and documented.



Key Points

- Investigation must be properly planned and structured.
- Wherever possible, an independent person should be appointed to carry out the investigation who is not part of the decision-making process in any subsequent disciplinary hearing.
- For serious cases (major misconduct), consider suspending the employee on pay during investigation.
- Investigation should be approached with an open mind.
- The employee whom the allegation has been made is interviewed, it should be made clear to the person that it is a facts-gathering interview and not a disciplinary hearing.
- It is not necessary to prove “beyond reasonable doubt”. The civil standard of proof (“on the balance of probabilities”) is acceptable standard.

Key concepts

- Whistleblowers at the heart of process
- Setting the tone – leaders as role models
- Engaging positively - no matter the outcome
- Responding to lead indicators

Summary

For WB to work,

- TRUST in the process must be established.
- Investigation must be objective, impartial, timely, factual and confidential.
- Fair and consistent sanctions if there is misconduct.