Common Investigation Issues

Gerry Zack, CCEP, CFE, CIA
CEO
Society of Corporate Compliance and Ethics
Minneapolis, MN, United States
gerry.zack@corporatecompliance.org

An Improperly Performed Investigation Creates More Risk Than it Mitigates
Issues in Every Phase of an Investigation

1. Initial phases of an investigation
2. Performing the investigation
3. Close out, reporting, and follow-up actions

PART 1

Initial Phases of an Investigation
Does it Matter What Triggered the Investigation?

Every Investigation is Different:
- Allegation/tip
  - Anonymous v. known
  - Internal v. third party
  - Level of specificity
- Internal audit or other auditing/monitoring activity
- External process (government auditors, etc)
- How serious is the alleged or possible act?
  - Escalation issues?

Allegations
- Perform preliminary assessment to determine whether an investigation is warranted
- Consider whether it is necessary to perform without subject’s knowledge (Covert v Overt)
- Data analytics can help in establishing need for investigation
  - Consider this – If the allegation is true, what impact would the act have on electronic data? How would the digital trail of the act differ from that of a valid transaction or act?
- Document analysis
  - Look for red flags, characteristics that support or refute the allegation
What Next?

- What type of compliance issue?
  - Bribery, conflict of interest, employee theft, fraud, privacy, data breach, environmental, financial reporting fraud, etc

- What level within the organization is implicated?
- Possible next steps:
  - If there is an allegation, assess credibility
  - Notify/engage legal counsel
  - Assemble team; Determine who investigates
  - Is subject currently employed with us?
    - Consider whether it is necessary to investigate without subject’s knowledge

Scope Considerations

- How specific/vague is the allegation or concern/red flag?
- Could additional individuals be involved?
  - Internal
  - Third parties (individuals or organizations)
- What other acts could the subject(s) have perpetrated?
  - Very common that if someone is engaged in wrongdoing, there are multiple schemes/acts
  - Perform role-based risk assessment
- How far back might the activity have been occurring?
- Are violations/losses potentially still occurring?
- How likely is it that other individuals may have witnessed the alleged wrongdoing?
What are the Goals of the Investigation?

- Stop certain conduct?
- Terminate an employee?
- Stop the bleeding?
- Civil litigation to recover damages?
- Refer for criminal prosecution?
- Keep it quiet?

Goals as Compliance Professionals

- Investigate processes, not people
- Ultimate goal is to find and fix the problem
Identifying Records & Data Needed

- Develop process map of the transaction/activity cycle(s) involved in the target of the investigation
  - MUST understand how the transaction cycle operates in order to identify relevant records/people needed
- Based on this process map, identify:
  - People involved in each step
  - Internal controls
    - Preventive
    - Detective
  - Documents and forms
    - Received
    - Created
  - Electronic records
  - Systems and databases affected

Example – For corruption in the purchasing cycle:
- Identification and documentation of need
- Development of specifications, if necessary
- Solicitation of bids or negotiation with alternative vendors
- Selection of vendor
- Contract, statement(s) of work, etc
- Purchase orders
- Change orders, subcontracts, etc
- Receipt of goods or services
- Submission, review and approval of invoice
- Payment
- In addition, what other internal records would we expect along the way? E-mails, electronic approvals, etc.
PART 2

Performing the Investigation

What Skills are Needed?

- Digital evidence (gathering/preserving)
- Interviewing
- Subject matter expertise
- Forensic accounting
- Damages calculations
- Data analytics
- Process & internal controls analysis
- Document analysis
- Records management, eDiscovery
Preserving/Collecting Electronic Evidence

• Issue a document/record hold notice based on process map explained earlier
  ▪ Identify relevant records
  ▪ Identify relevant record custodians (may include third parties, cloud storage, etc)

• Negative implications of information being lost/altered

• ESI (electronically stored information):
  ▪ What ESI is relevant?
  ▪ What format is it in?
  ▪ Where is relevant ESI stored?
  ▪ How do we ensure we collect it all?
  ▪ Proper collection (use forensically recognized technologies)

Case Management

• Misplaced or unorganized documents and records
  ▪ Security and indexing/tagging
  ▪ Sources of documents and data

• Losing track of or never properly documenting sequence of events
  ▪ Maintaining the timeline
The Tainted Witness

• How do you deal with a witness who provides useful evidence, but who comes with their own baggage
  • Past or pending disciplinary issues
  • Possible involvement in the issue you are investigating

PART 3

Reporting and Following Up
Reports – Who Are the Readers?

- Internal; Management
- Board of Directors
- Third Parties (funding sources, customers, etc)
- Government Agencies, Regulators, etc
- Public
- Judges, Jurors, Opposing Counsel

Common Report Issues

- Clerical/typos
- Rambling, stream of consciousness narrative
  - It makes sense to you – and only you
- Assuming knowledge of the reader
- Omitting exculpatory evidence
- Too many drafts or supplemental materials
QUESTIONS ??

Gerry Zack, CCEP, CFE
CEO
Society of Corporate Compliance and Ethics
Tel: +1 952.567.6215
gerry.zack@corporatecompliance.org