

Common Investigation Issues

Gerry Zack, CCEP, CFE, CIA

CEO

Society of Corporate Compliance and Ethics

Minneapolis, MN, United States

gerry.zack@corporatecompliance.org



1


An Improperly Performed Investigation Creates More Risk Than it Mitigates



2

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



3

PART 1

Initial Phases of an Investigation



4

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?



5

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



6

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



7

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?



8

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?



9

Goals as Compliance Professionals

- Investigate processes, not people
- Ultimate goal is to find and fix the problem



10

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




11

Identifying Records & Data Needed


- **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.



12

<h1>PART 2</h1> <h2>Performing the Investigation</h2>	
 SCCE™ Society of Corporate Compliance and Ethics	

13

<h1>What Skills are Needed?</h1>	
<ul style="list-style-type: none">• Digital evidence (gathering/preserving)• Interviewing• Subject matter expertise• Forensic accounting• Damages calculations• Data analytics• Process & internal controls analysis• Document analysis• Records management, eDiscovery	
 SCCE™ Society of Corporate Compliance and Ethics	

14

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)



15

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



16

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



17

PART 3


Reporting and Following Up



18

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



19

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



20

QUESTIONS ??

Gerry Zack, CCEP, CFE

CEO

Society of Corporate Compliance and Ethics

Tel: +1 952.567.6215

gerry.zack@corporatecompliance.org

