23rd May 2023

ALJB | The Luxembourg Banking & Financial Law Association

Discovering smoking guns – the conduct of forensic investigations

Speaker:
Elisabeth Omes

Partner
Elvinger Hoss Prussen

Speaker :
Philippe Dupont

Partner
Arendt & Medernach S.A

Speaker :
Michael Weis

Partner
PwC Luxembourg

Definition

- **Multiple types of forensic investigations**
- **Main object:**
  - gathering and analysis of evidence (i.e. establish facts) in order

    (i) to reach a conclusion

    (ii) to respond to a request of an authority

    (iii) to prepare the defense or action in a case
- **Key components**
  - preservation and integrity of data
  - traceability / chain-of-custody
  - legality of data gathering and analysis

(i) to reach a conclusion

- **Context**
  - internal investigation, e.g.
    - following a whistleblowing
    - information on harassment
    - greenwashing allegation
- **Action**
  - data gathering, e.g.
    - written communications (forensic technology)
    - interviews

(ii) to respond to a request of an authority

- **Context**
  - external investigation, e.g.
    - following a request of a supervisory authority (CSSF, CAA, foreign authorities)
    - in the context of a criminal investigation
- **Action**
  - data gathering, e.g.
    - written communications (forensic technology)
    - interviews
    - forensic accounting
    - forensic IT

(iii) to prepare the defense or action in a matter

- **Context**
  - regulatory investigation
  - criminal investigation
  - civil law action
- **Action**
  - data gathering
    - written communications (forensic technology)
    - data restoration (forensic IT)
    - interviews
    - forensic accounting
    - corporate intelligence
    - asset tracing

Setting up the investigation team (I)

- **Selection principles:**
  - Neutrality:
    - avoid accusation of bias: the conclusions must be a fair assessment of the facts
  - No conflicts of interests:
    - Investigators should not have a self-interest in the investigated matter
  - Experience
    - Investigators should have a extensive experience in the investigated matter for reaching defensible conclusions
  - Resources
    - Investigations are time-consuming; investigation teams must be adequately staffed

Setting up the investigation team (II)

- **Use of external specialists**
  - When are external specialists required?
    - Misconduct is widespread
    - Misconduct may involve management or board members
    - Misconduct may lead to regulatory sanctions or judicial actions
    - Lack of internal resources (staff is needed to run their departments; IT)
- **Benefits of external investigators**
  - Absence of roadblocks for the conduct of the investigation
    - Skills and experience
    - Work relationships
  - Confidentiality and professional secrecy

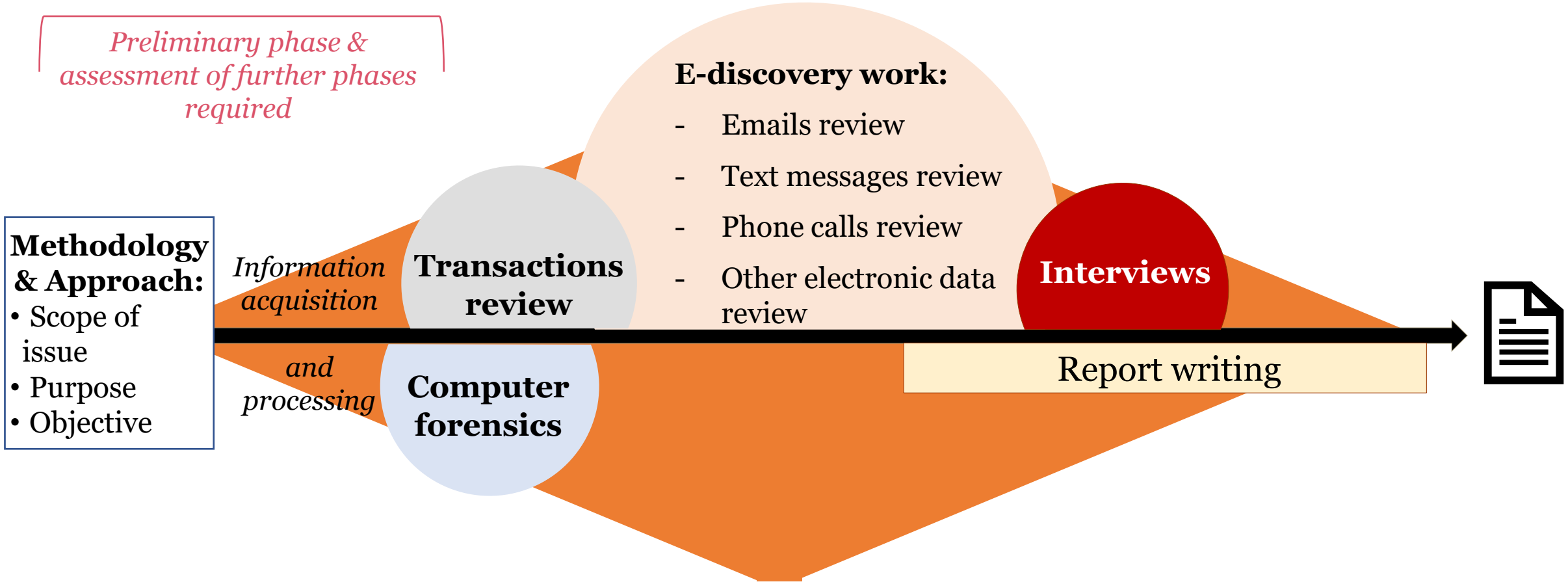
Setting up the investigation team (III)

- **Involvement of internal resources**
  - Internal audit
  - Legal & Compliance
  - HR
  - Management
  - Independent directors

- **Use with caution**
  - Tension at the workplace
  - Workload

Conceptual view on conduct of the investigation

Preliminary phase & assessment of further phases required



Work divided into phases and workstreams based on the preliminary assessment. May be adjusted based on intermediary findings.

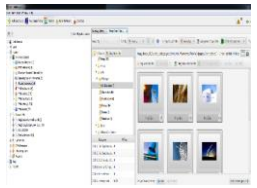
How do we do it?

Key pillars of a forensic investigation

Report

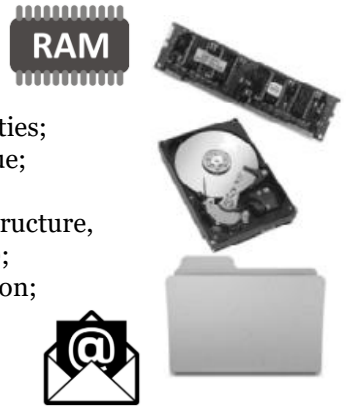
- Report findings (Factually);
- Propose recommendations and insight;

Investigate



- Interview;
- Analyze logs;
- Analyze malwares;
- Review and tag hits;
- Profile account usage;
- Identify unusual patterns;
- Analyze relevant artefacts:
  Browsing activity, Thumbnails, Apps, …
- Search for indicators of compromise;

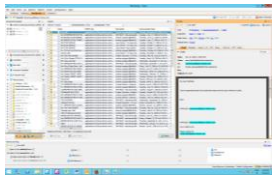
Scope



- Discuss with the client and involved parties;
- Understand what happened and the issue;
- Understand the client needs;
- Understand the environment (IT infrastructure, Applications, business and IT processes);
- Request relevant data for the investigation;

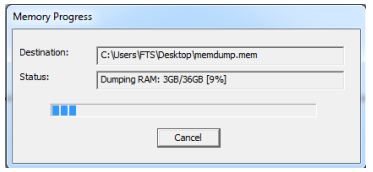
Process & Extract

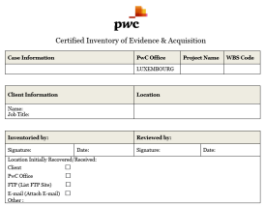
- Triage and data extraction
- Process evidences
- Restore deleted files
- Search and profile



Data sources

Phones, SIM	Cars, GPS	Mail boxes
Hard drives	Logs (network, …)	File servers
Live memory	External storage media	





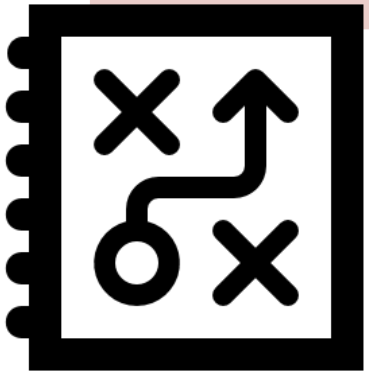
Investigation Life-Cycle

Strategy & Planning

Evidence Gathering

Analysis & Interviewing

Reporting & Closure



Investigation Life-Cycle

It happened – 4 things to do first…

1a.Activate the incident team: Specialists, trained staff and external support (legalcounsel, forensicinvestigator, communication)

1b. Safeguard potential evidence: Documents, electronic data, communications etc. BUT do it right!

2. Deal with the suspected employee.

3. Other considerations about insurance, compliance and reporting etc. depends on the case

Strategy & planning

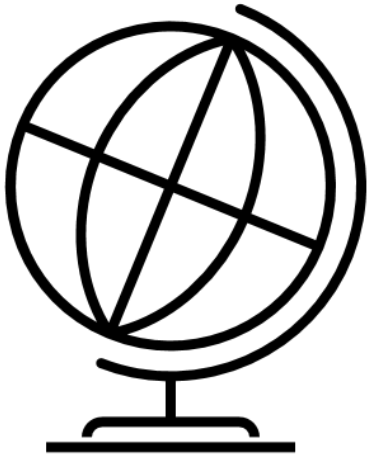
Key areas to consider

- ***5W1H* or**

  WHAT – WHY – WHO – WHERE – WHEN – HOW

  - What has happened? What are the client's objectives? What does the client need from us?
  - Why is the investigation done? Why did it happen?
  - Who did it? Who am I reporting to?
  - Where did it happen? Where is the mandate coming from?
  - When did it happen? When was it discovered?
  - How will our work be used? How will I investigate?

- Different types of investigations (e.g. corroborate evidence, find out why/why-not, fact finding, expert opinion)
- Legal considerations



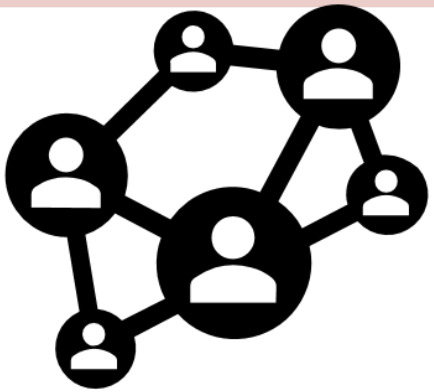
Investigation Life-Cycle

Strategy & Planning

Evidence Gathering

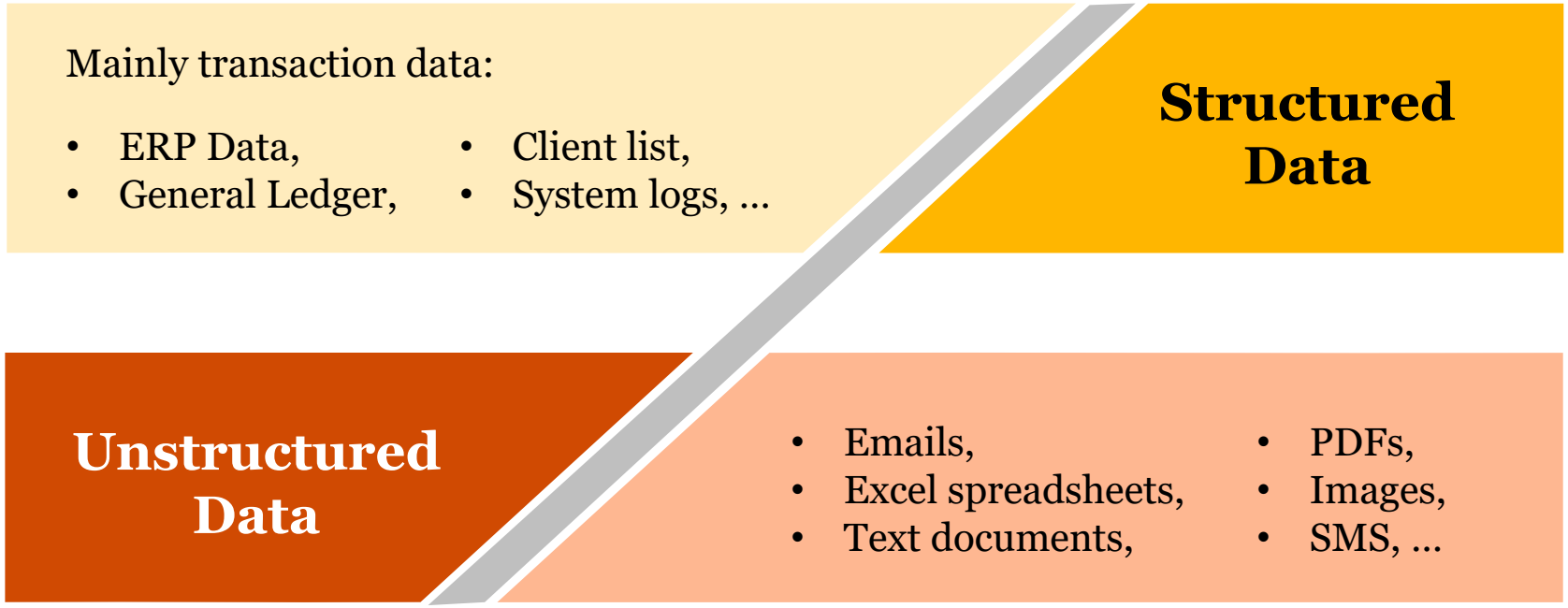
Analysis & Interviewing

Reporting & Closure



Evidence gathering - data complexity

Structured Vs. Un-structured data



A major challenge is to process data in order to structured them for an easier review

Evidence gathering - our approach

- Scope definition
- Data structure understanding
- Data collection

pwc  

- Data preparation and loading
- Verification of the completeness
- Data validation

pwc 

- Data organisation / partitioning
- Identification of key documents to investigate

pwc

- Result review and evaluation
- Advanced search: find linked documents

pwc  

- Show dependencies and models
- Prepare the data: make it interactive and easy to understand

pwc 

Forensic investigation may sometimes be « mandatory »

- duty to cooperate (Article 40, 1993 Law on the financial sector)
- harassment (Article L 246-3, Code du travail – Law 29 March 2023)
- whistleblowing (Law 16 May 2023 – Article 7)
- certain criminal investigations (bill of law n° 8051 – new Article 66(8) – Code de procédure pénale)
- Corporate sustainability due diligence directive - draft

Enquiries by Administrative Authorities

- CSSF / CAA: duty to cooperate
- sanctions in case of failure to cooperate
  - monetary sanctions
  - aggravating factor
- criminal law risk (Article 23 (2) CPP)

   tension cooperation >< sanction risk
- forensic enquiry
  - context of cooperation
  - preparation defense

Criminal Law Investigations

- data seizure
  - global seizure
  - targeted seizure

- bridge information gap
- preparation of defense strategy
- forensic investigation
  - forensic technology
  - forensic IT
  - corporate intelligence

Can prevention measures be taken? (1/3)

Preventing and detecting Financial Crime is a complex challenge.

Predicate offense vs. Secondary offense?

What is a predicate offence?

A predicate offence is a component of a more serious criminal offence.

Example of offences which are predicate offences to money laundering & terrorist financing:

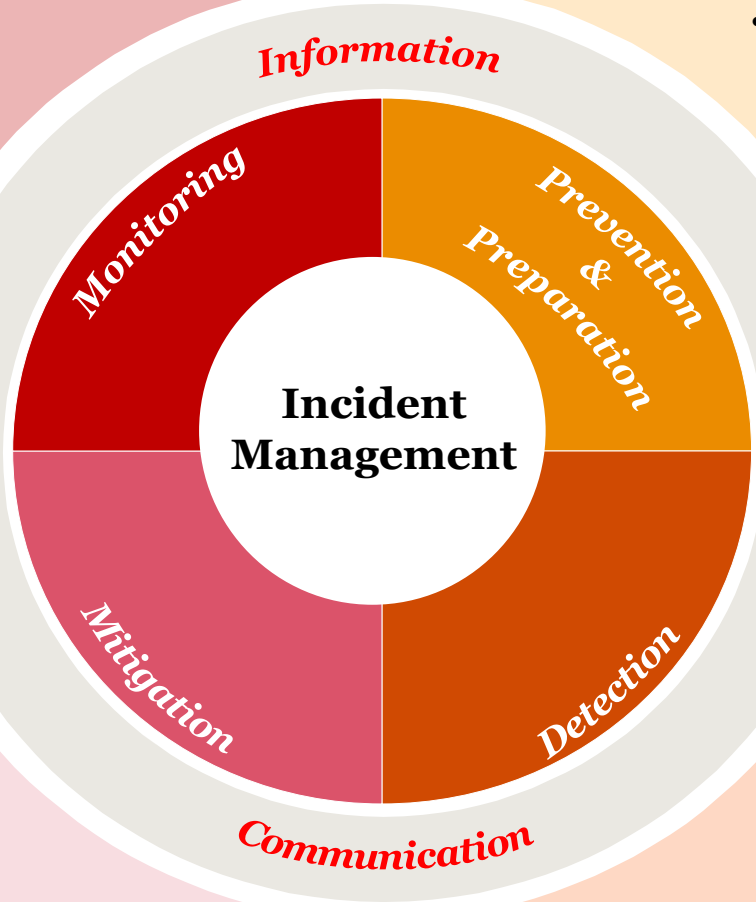
Corruption; Human, Narcotics and Arms Trafficking; Fraud; Tax Evasion; Insider trading & market manipulation.

Can prevention measures be taken? (2/3)

Overview of action areas of a robust anti-fraud management system

- IT & Data monitoring
- Regular reporting
- Internal audit
- Business Partner Due Diligence or KYC
- Compliance oversight

- Procedures & Incident management approach
- Data segregation & device usage concept
- Trainings & Awareness
- Good Governance
- Risk assessment



- Crisis Management
- Communication strategy
- Investigation and follow-ups
- Process review and optimization

- Internal Controls structure
- Whistleblowing
- Anti-Fraud Review
- Data analytics

- Regular communication to employees
- Feedback channels

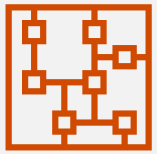
Can prevention measures be taken? (3/3)

“You don’t know what you don’t know”
- Michael Weis

A fraud risk assessment is an **effective tool** utilized to **identify and prioritize areas of fraud risk** within their organisation.

It includes:

- Inherent Risk Assessment
- Mitigating Controls Assessment
- Residual Risk Assessment



Based on the remaining residual risks, a company can decide to:

- Avoid the risk
- Transfer the risk
- Mitigate the risk, or
- Assume the risk.

Legal issues to be borne in mind (I)

- **Clients**
  - Check your General Terms & Conditions
    - Data protection clauses and use/transfer of data
    - Recorded telephone lines and cameras
  - Confidentiality of client data
    - How to handle targeted clients
    - How to protect non targeted clients

Legal issues to be borne in mind (II)

- **Protection of employees**
  - Data protection
    - Investigation of emails and devices
  - Whistleblowing
    - Investigation of the incident, not the whistleblower
  - Harassment
    - Impartial and rapid investigation of the facts
  - Labour law:
    - Immediate dismissal
    - Dismissal with notice
    - Leave of absence

Legal issues to be borne in mind (III)

- **Insurance**
  - Is the incident covered?
  - Report the incident to the insurer

- **Anticipate litigation**
  - Civil claims
  - Regulatory actions
  - Criminal investigations
  - Labour law

ALJB | The Luxembourg Banking & Financial Law Association

Thank you for your attention

–

Q&A

Speaker:
Elisabeth Omes

Partner
Elvinger Hoss Prussen

Speaker :
Philippe Dupont

Partner
Arendt & Medernach S.A

Speaker :
Michael Weis

Partner
PwC Luxembourg