



**Forensic Auditing Manual
for the
Audit Office of Guyana**

Preface

The Audit Office of Guyana (AOG) is the country's Supreme Audit Institution and performs a very significant role in ensuring transparency in, and the integrity of, spending by public financial systems within the jurisdiction. In the development of its investigative capacity, the AOG in 2008 established a Forensic Audit Unit which functions to fully investigate matters referred to it and reports to the Auditor General with recommendations. The Forensic Audit Unit was established under Regulation 8 of Regulations made under Section 11 of the Guyana Audit Act 2004. Institutional strengthening is an ongoing process, which include the need to enhance investigative capabilities.

In anticipation of the economic impact from the significant oil revenues being generated since December 2019, it is now considered imperative that Guyana's government business practices are reviewed and reformed, with an emphasis on the capabilities and integrity of regulatory agencies such as the Audit Office of Guyana (AOG) that have a defined role in the oversight of Budget Execution in the public sector.

The resultant changes in the oversight responsibilities of the AOG has created an impetus for the enhancement of its investigative capabilities to safeguard the public trust and improve the efficiency in the use of public resources. Accordingly, the AOG has identified the need to improve its application and use of forensic investigative skills to unearth fraudulent activity, embezzlement, and other financial irregularities.

Further, as the scope of forensic auditing has expanded exponentially, especially as many use the internet as a medium to conceal illegal transactions, the skill of evidence gathering and analyzing data through technology has become an area of special interest to the AOG. In improving the relevant skill sets in executing forensic and/or special audits the AOG will be positioned to create effective strategies to counter, detect and successfully investigate potential cases of fraud, providing useful and timely recommendations to its stakeholders and auditees, prompting corrective action by anti-corruption agencies/bodies.

In this context, the Inter-American Development Bank (IDB) commissioned a Consultancy to improve the Forensic Audit Capacity within the Supreme Audit Institution of Guyana. The

consultancy was tasked with delivering a training programme with an emphasis on the identification of systematic risks and fraudulent activities, forensic auditing techniques, approaches and court proceedings. The training to be complemented by refining/development of a forensic audit manual for the AOG, in accordance with ISSAI requirements.

The Caribbean Institute of Forensic Accounting (CIFA), engaged as consultants to execute the commission, has delivered the required training and produced this Forensic Audit/Accounting Manual.

Table of Contents

Introduction.....	5
Chapter 1: Understanding Financial Investigations	18
Chapter 2: Assembling an Investigation Team	27
Chapter 3: Investigatory Planning Checklist	29
Chapter 4: Using Case Management Software	33
Chapter 5: Choosing Investigative Methods and Techniques.....	36
Chapter 6: Investigating Corruption	41
Chapter 7: Building Coordination and Cooperation Networks.....	46
Chapter 8: What is Evidence	50
Chapter 9: The Gathering of Information and Evidence	53
Chapter 10. The Gathering of Private Digital Sources of Evidence and The Use of Digital Forensic Tools.....	69
Chapter 11: Human Intelligence	78
Chapter 12. The Gathering and Analysis of Financial and Corporate Evidence	84
Chapter 13: The Basic Steps of a Complex Fraud and Corruption Investigation.....	94
Chapter 14: Conducting Effective Interviews.....	98
Chapter 15: Investigative Report Writing	107

Introduction

The Audit Office of Guyana

The Office of the Auditor General is established by under Article 223 of the Constitution of the Republic of Guyana. The Constitution also secures the independence of the Office, describes its principal functions, and articulates provisions to govern the appointment of the Auditor General.

The Audit Office of Guyana scrutinises the expenditure of public funds on behalf of Parliament, and this includes audits of public corporations, statutory bodies, all central and local government entities, all bodies and entities in which the State has a controlling interest; and all projects funded by way of loans or grants by any foreign state or organisation and trade unions.

The Auditor General must submit annual reports to the Speaker of the National Assembly, who causes them to be laid before the National Assembly.

The Audit Act (2004) of the Laws of Guyana as amended, specifies the duties and powers of the Auditor General in relation to central government agencies and other entities in which the State has a controlling interest.

Section 24(2) of the Audit Act set out the following general objectives:

“In conducting financial and compliance audits, the Auditor General shall examine in such manner as he deems necessary the relevant financial statements and accounts and ascertain whether:

- a) The financial statements have been properly prepared, in accordance with applicable law, and properly present the operations and affairs of the entity concerned;
- b) The accounts have been faithfully and properly kept;
- c) The rules, procedures and internal management controls are sufficient to secure effective control on the assessment, collection and proper allocation of revenues;
- d) All moneys expended and charged to an account have been applied to the purpose or purposes for which they were intended; and

- e) Essential records are maintained, and the internal management controls and the rules and procedures established and applied are sufficient to safeguard the control of stores and other public property. ...”

Section 11 of the Audit Act empowers the Auditor General, with the approval of the Public Accounts Committee, to make Regulations for the proper administration of the Act, and such Regulations may include a Rules, Policies and Procedure Manual. Under Regulation 8(1) the Auditor General established a Special Investigations Unit within the Audit Office to deal with issues of financial misconduct. The Audit Office also has in place a Rules, Policies and Procedure Manual which under Paragraph D.4.1 state that this Unit shall engage staff specially trained in investigating fraud and corruption and familiar with the standards of criminal as well as audit evidence.

Para D.4.1.1 of the said Manual further states that:

“When, in the course of completing a financial, compliance or performance audit, the Auditors discover what they believe to be criminal fraud and corruption, they shall immediately notify the Auditor General and the Head of the Special Investigations Unit.

The Auditor shall determine if the case should be assigned to the Special Investigations Unit for further examination. After completing their examinations, if the Special Investigations Unit determines that sufficient evidence exists to warrant criminal investigation and prosecution, they shall ask the Auditor General to refer the case to the Police and appropriate judicial authorities.”

These actions are required by Regulation 8(2) under which: -

“... the Unit shall investigate the matter and submit a report with recommendations to the Auditor General who, where a criminal offence has been committed shall refer the matter to the Director of Public Prosecutions and send a copy to the Commissioner of Police for appropriate action.”

Sections 30 to 34 of the Audit Act as amended speaks to the duties and, in the context of conducting special investigations, powers of the Auditor General in

relation to central and local government agencies, and other entities in which the State has a controlling interest.

For ease of reference, and because of their importance to the performance of special investigations, the provisions of Sections 30 to 34, which are clear and unambiguous, are detailed in full below:

“Requirement to provide information

S.30 The Head of a budget agency, or the governing body in the case of other public entities, shall ensure that the Auditor General has access at all reasonable times to the documents of the budget agency or entity relating to the discharge of the Auditor General’s functions. This shall include providing reasonable, suitable and secure space for the Audit Office to conduct its work. The Head of a budget agency or governing body shall also furnish the Auditor General from time to time or at regular periods, as may be specified by the Auditor General, with the accounts of the transactions of the budget agency or entity.

Power to obtain information

31. For the purpose of the discharge of his functions, the Auditor General may require a public entity, or any officer or employee of a public entity, to -

- (a) produce a document in the entity’s or person’s custody, care or control; and*
- (b) provide the Auditor General with information or an explanation about any information.*

Power to obtain evidence

32. The Auditor general may, in the course of the discharge of his functions, require a person to give evidence either orally or in writing.

Power to inspect bank accounts

33. For the purpose of the discharge of his functions, the Auditor General may examine or audit the account of any person in any bank if the Auditor General has reason to believe that moneys belonging to a public entity have been fraudulently or wrongfully paid into such person’s account, except that -

- (a) *to exercise this authority, the Auditor General shall establish that information obtained shall not be used for any purpose other than intended and shall first obtain a warrant from a court authorizing such examination.*
- (b) *when presented with the warrant, the bank through its officer shall produce any documents or provide requested information relating to the relevant account; and*
- (c) *the Auditor General may make copies of any documents so produced.*

Access to premises

34. *For the purpose of obtaining documents, information or other evidence relevant to any matter arising in the discharge of his functions, the Auditor General or any officer so authorized by him may, at all reasonable times and with proper identification*
- (a) *enter into and remain on a public entity's premises;*
 - (b) *enter into and remain on any other premises if so authorized by a warrant issued by a court on the grounds that there is reason to believe that documents or other information relating to the activities of a public entity may be held at those premises; and*
 - (c) *carry out a search for documents, examine documents, or make copies of documents."*

These sections should very significantly facilitate the Special Investigations Unit when undertaking its function. They allow the Auditor General, subject to the limitations in Sections 33 and 34(1)(b) where a warrant is required, virtually unimpaired access to public premises, all documents and staff members falling within the AOG's remit.

The Concept of Fraud

Fraud is one of the biggest and most damaging risk governments face. It is not unusual to see headlines about public (and for that matter private) sector organizations being affected by fraud. The consequences of fraud on the country may be devastating and can result in among others:

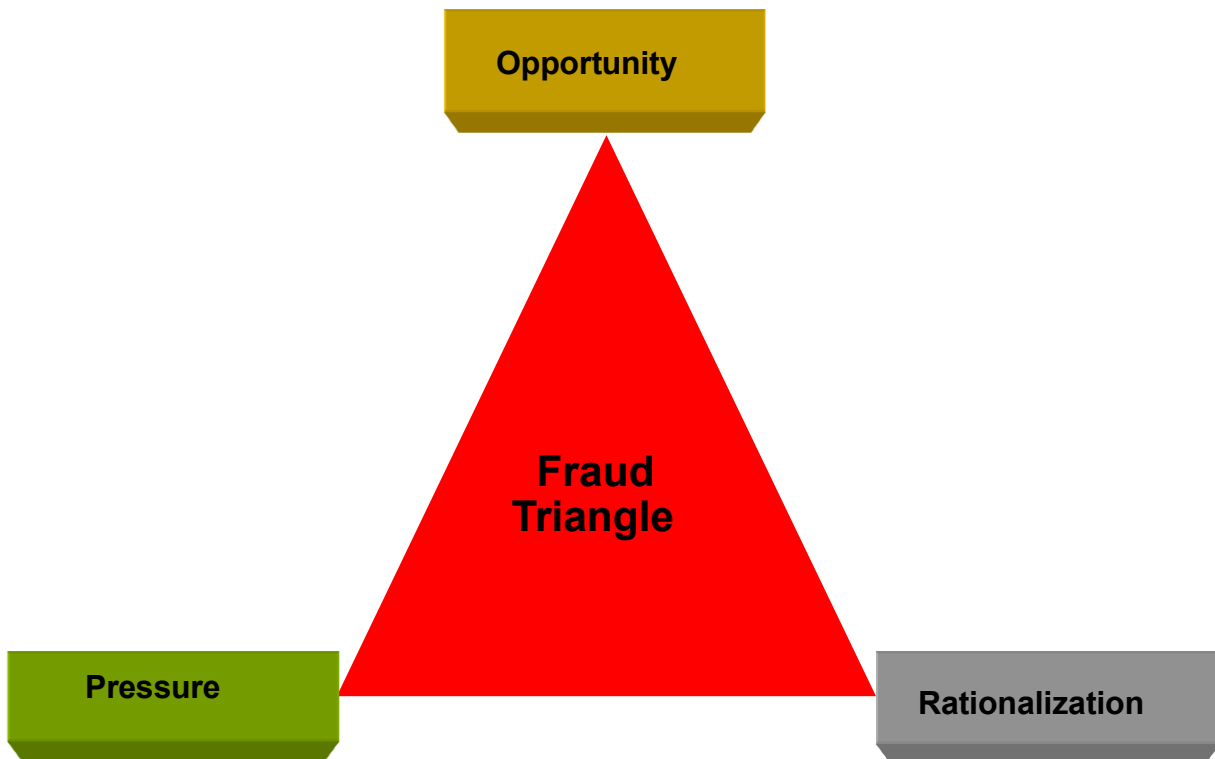
- Low foreign investment and trade,
- Inefficient allocation of resources,

- Poor education and healthcare, and
- Undermine democracy and the rule of law.

Fraud may be defined as wrongful or criminal deception intending to result in financial or personal gain. The Association of Certified Fraud Examiners describe fraud in terms of occupational frauds and classifies fraud into three primary categories: Asset Misappropriations, Corruption and Financial Statement Fraud.

The Fraud-Triangle and the Fraud Diamond

As indicated, fraudulent schemes vary in scope and context especially with the position of the perpetrators within an establishment. The fraud triangle and the fraud diamond are two models employed to explain the factors that cause someone to commit occupational fraud. The fraud triangle model consists of three components leading to fraudulent behaviour. They are pressure, opportunity and rationalization (see diagram below).



I. Pressure

This is the first motive in the Cressey fraud-triangle hypotheses. It describes the strong financial needs that is usually too personal and for which an individual is ashamed to make public. The perpetrator is unwilling to share his need with others, therefore may not receive help from friends and relatives.

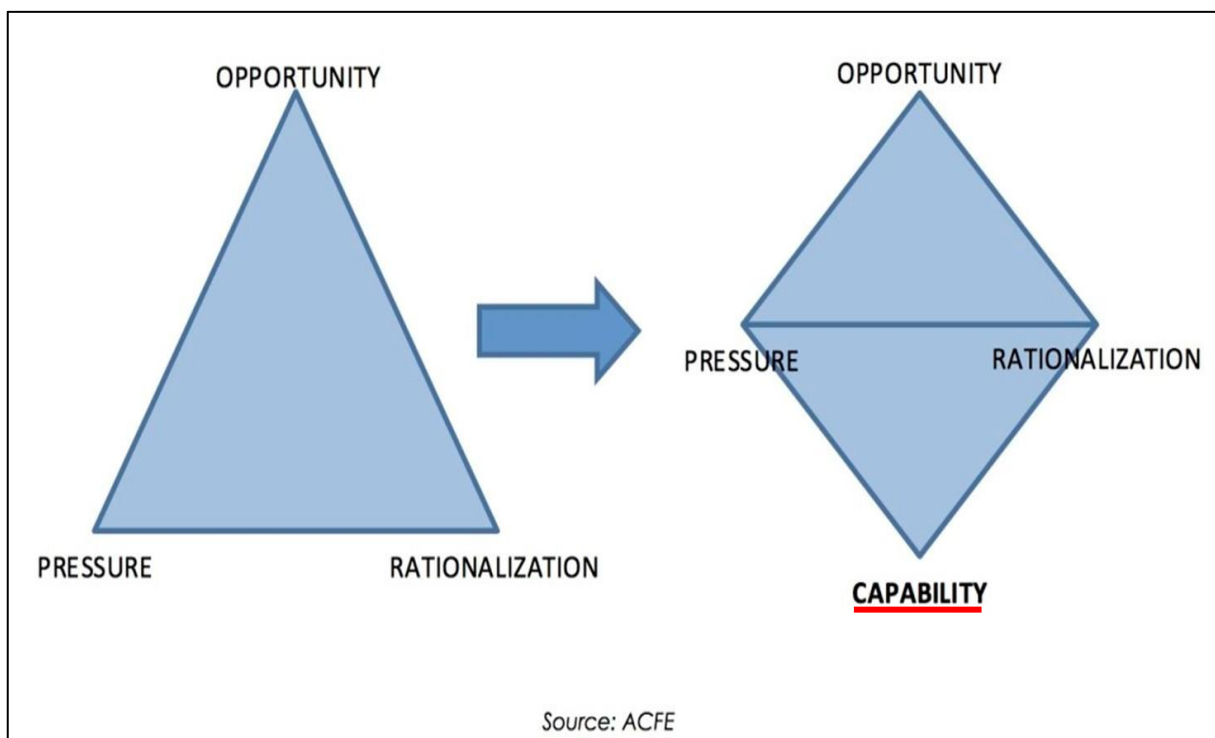
II. Opportunity

This usually occurs when there is lack of internal controls within an organization. The fraud committer may take advantage of the situation with the knowledge that he may not be caught. Opportunity within a job function is tied to poor internal control system.

III. Rationalization

The third motive in fraud-triangle hypotheses is the perpetrator's mindset. The perpetrator has conditioned his mind that what he did was not wrong. This action is seen as smartness instead of illicit activity.

The Fraud Diamond



Experts now believe that the fraud triangle could be enhanced by considering a fourth factor that explains why fraud occurs, this is capability.

Capability

This is the situation of having the necessary traits or skills and abilities for the person to commit fraud. It is where the fraudster recognised the particular fraud opportunity and ability to turn it into reality. Position, intelligence, ego, coercion, deceit and stress, are the supporting elements of capability. The theory believes that frauds would not have occurred without the right person with right capabilities implementing the details of the fraud. In essence the fraud diamond moves beyond viewing fraud opportunity largely in terms of environmental or situational factors.

The vulnerability that an organization has to those capable of overcoming all fraud elements of the fraud triangle and the fraud diamond are fraud risks. Fraud risks can come from sources both internal and external to the organization.

Forensic Accounting/Audit Tool and Techniques

Forensic accounting is a field of accounting that employs accounting practice, auditing and investigative skills to uncover fraud, embezzlement, hidden assets and other financial irregularities. Forensic accounting is evidentiary in nature, concerned with uncovering all types of financial fraud, including detection of financial misrepresentation and financial statements fraud.

It provides analytical evidence suitable for use in court during legal proceedings. Audit techniques and procedures are used to identify and to gather evidence to prove, for example, how long fraudulent activities have existed and carried out in the organization, and how it was conducted and concealed by the perpetrators. The efficacy of forensic accounting in providing evidence for use in court lays on its ability to integrate an understanding of accounting principles with investigative procedures. Forensic accounting experts are often asked to provide litigation support where they are called on to give expert testimony about financial data and accounting activities.

Forensic Auditing comprises three key ingredients:

I. Forensic Audit Thinking

involves the critical assessment throughout the audit of all evidential matter and maintaining a higher degree of professional scepticism that, for example, fraud or financial irregularity may have occurred, is occurring, or will occur in the future. Furthermore, Forensic thinking is a mind shift where the auditor believes that the possibility of fraud or financial irregularity may exist, and the controls may be overridden to accomplish that possibility. Forensic thinking is used throughout the audit work i.e., from start to finish.

II. Forensic Audit Procedures (both proactive and reactive)

These are more specific and geared toward detecting the possible material misstatements in financial statements resulting from fraudulent activities or error. Audit procedures should align with Fraud Risks and Fraud risk Assessments.

A fraud risk assessment is a powerful proactive tool in the fight against fraud for any organization. According to the Association of Certified Fraud Examiners (ACFE), Fraud Risk assessment is a process aimed at proactively identifying and addressing an organization's vulnerabilities to internal and external fraud. It is important regard a fraud risk assessment as an ongoing, continuous process, rather than just an activity. A fraud risk assessment starts with an identification and prioritization of fraud risks that exist in the organization.

Accordingly, the fraud examiner/investigator should have the following skills:

- (i) an investigative mindset which should be more than skeptical,
- (ii) An understanding of fraud schemes termed as occupational fraud (Corruption, Asset Misappropriation and Financial statement fraud),
- (iii) Experience in dealing with fraud issues,
- (iv) Knowledge of investigative, analytical, and technology-based techniques (Digital or computer forensics, e.g., how to gather, analyze and interpret data), and
- (v) Knowledge of legal processes.

Additionally, on *Forensic Audit Procedures*, the following are recognized investigative tools and techniques used by forensic specialist/fraud examiners.

- (i) Review of Public document and background investigations,
- (ii) Interviewing of knowledgeable persons (witness(es) and the accused),
- (iii) Confidential sources and informants,
- (iv) Laboratory analysis of physical and electronic evidence (Physical Forensic Analysis which includes Handwriting analysis, fingerprint analysis, document dating, ink sampling, simulated forgery of signatures analysis, Computer Forensics which includes hard disk imaging, E-mail analysis, search for erased files, analyze use & possible misuse of office computers for personal use, ensure chain of custody for electronic evidence,
- (v) Electronic and physical surveillance,
- (vi) Undercover operations, and
- (vii) Analytical procedures (Using of Ratio analysis, Trend or time series analysis, Horizontal and vertical analysis and use of work-back ratios techniques to analyze financial statement).

III. Appropriate Use of Technology – Forensic Data Analysis

Forensic Data Analysis can be used to Prevent, detect, control fraud and other irregularities. It may be described as the process of gathering, summarizing, comparing, and aggregating existing different sets of data that organizations routinely collect in the normal course of business with the goal of detecting anomalies that are traditionally indicative of fraud or other misconduct.

The following are some of the benefits of using forensic data analysis tools and techniques:

- (i) Analyzes 100% of data sets rather than using statistical sampling,
- (ii) Identification of potential control environment weaknesses,
- (iii) Facilitates assessment of the effectiveness of existing anti-fraud and fraud risk management programs and practices,
- (iv) Facilitates identification of potential policy and process violations,
- (v) Vendor acceptance/approval processes, Bid tailoring, etc,
- (vi) Facilitates interviews in investigations.

TYPES OF INVESTIGATIONS

The forensic auditor may have to investigate many different types of fraud, which can be categorized into three groups to provide an overview of the wide range of investigations that could be carried out. The three categories of frauds are;

- i. Corruption,
- ii. Asset Misappropriation and
- iii. Financial Statement Fraud

Corruption

Corruption is any unlawful or improper behaviour that seeks to gain an advantage through illegitimate means, e.g., Bid Rigging and Price manipulation. There are three types of corruption frauds: conflicts of interest, bribery, and extortion.

- In a conflict-of-interest fraud, the fraudster exerts their influence to achieve a personal gain which detrimentally affects the organization.
- Bribery is giving or receiving an unearned reward to influence another person's behavior
- Extortion is the opposite of bribery and happens when money is demanded (rather than offered) in order to secure a particular outcome.

Asset Misappropriation

This involves third parties or employees in an organization who abuse their position to steal from it through fraudulent activities. There are many different types of fraud which fall into this category. The most common feature is the theft of cash or other assets from an organization through, for example:

- Embezzlement – the wrongful taking or conversion of the organization's property by a person to whom it has been lawfully entrusted.
- Cash theft – the stealing of physical cash from the organization premises.
- Fraudulent disbursements – organization funds being used to make fraudulent payments.
- Inventory frauds – the theft of inventory from the organization's stock/store.
- Misuse of assets – staffs using organization's assets for their own personal interest.

Financial Statement Fraud

This is also known as fraudulent financial reporting; this is a type of fraud that causes a material misstatement in the financial statements. It can include deliberate falsification of accounting records; omission of transactions, balances or disclosures from the financial statements; or the misapplication of financial reporting standards (IFRS, SAS, IPSAS). This is often carried out with the intention of presenting the financial statements with a particular bias, for example concealing liabilities in order to improve any analysis of liquidity and gearing.

Conducting The Investigation

The process and various stages of conducting a forensic investigation are briefly described below.

Accepting the Investigation

The forensic auditor or accountant must initially consider whether he/she has the necessary skills and experience to accept the work or in house competence of staffs. Forensic investigations are specialist in nature, and the work requires detailed knowledge of fraud investigation techniques and the legal framework.

Planning the Investigation

The investigating team must carefully consider what they have been asked to achieve and plan their work accordingly. The objectives of the investigation will include:

- (i) Identifying the type of fraud, life span, and how the fraud has been concealed by the fraudster(s) involved,
- (ii) Quantifying the financial loss suffered,
- (iii) Gathering evidence to be used in court proceedings, and
- (iv) Provide advice to prevent recurrence of the fraud.

Gathering Evidence

In order to gather detailed evidence, the investigator must understand the specific type of fraud that has been carried out, and how the fraud has been committed.

The evidence should be sufficient to ultimately prove the identity of the fraudster(s), the mechanics of the fraud scheme, and the amount of financial loss suffered.

It is important that the investigating team are skilled in collecting evidence that can be used in a court case, and in keeping a clear chain of custody until the evidence is presented in court. If any evidence is inconclusive or there are gaps in the chain of custody, then the evidence may be challenged in court, or become inadmissible.

Evidence can be gathered using various techniques, such as:

- Testing internal controls to gather evidence which identifies the weaknesses, which allowed the fraud to be perpetrated,
- Using analytical procedures to compare trends over time,
- Applying Computer Assisted Audit Techniques (CAATs) to identify the timing and location of relevant details being altered in the computer system,
- Discussions and interviews with staffs, and
- Substantive techniques such as reconciliations, cash counts and reviews of documentation.

The ultimate goal of the forensic investigation team is to obtain a confession by the fraudster, if a fraud did actually occur. For this reason, the investigators should avoid deliberately confronting the alleged fraudster(s) until they have gathered sufficient evidence to extract a confession. The interview of the suspected perpetrator(s) is a crucial part of evidence to be gathered during the investigation.

Reporting

For every outcome of an investigation there must be a report detailing the findings of the investigation which include a summary of evidence and a conclusion as to the amount of loss suffered as a result of the fraud. The report should also describe how the fraudster set up the fraud scheme, and which controls, if any, were circumvented. Finally, the reports should contain recommendations in order to prevent any similar frauds recurring in the future.

Court Proceedings

The investigation is likely to lead to legal proceedings against the suspect, and members of the investigative team will probably be involved in any resultant court case. The evidence gathered during the investigation will be presented at court, and team members may be called to court to describe the evidence they have gathered and to explain how the suspect was identified.

It is imperative that the members of the investigative team called to court can present their evidence clearly and professionally, as they may have to simplify complex accounting issues so that non-accountants involved in the court case can understand the evidence and its implications.

Chapter 1: Understanding Financial Investigations

The main aim of a financial investigation is to uncover, document and analyze where money comes from, how it is moved through financial institutions and how it is used or stored during the process of criminal activities. This practice, also known as forensic accounting, is commonly used for corporate investigations, embezzlement schemes, money laundering schemes, tax evasions, theft and various types of monetary schemes. It establishes the origin of fraudulent practices in financial transactions, reveals the beneficiaries, indicate the timeline associated with the transfer or conversion of cash obtained illegally and provides admissible evidence of financial criminal activities, which can be used in litigation. Beyond the financial damage suffered by the organization attacked, fraud can undermine investor confidence in an entire industry or can damage the economy of a country. Financial investigators are the legal, unbiased source who can play an important role in preserving or restoring financial stability in such cases.

To ensure the efficiency and effectiveness of financial investigations, the designation of powers to expert personnel to access data (including data from private and public sources) and applying special investigative powers are necessary, to obtain the evidence needed for criminal or civil proceedings against persons who commit financial crimes. Investigators use various tools and techniques to obtain evidence of financial anomalies and analyze relevant data to prove or dispel the assumption of fraudulent conduct.

It is noteworthy that under Sections 30 to 34 of the Guyana Audit Act (2004) (the Audit Act) the Auditor General and those he authorizes have power to enter any relevant government department, office or agency and must be given access to all documents, materials and staff (including for interview) during an investigation.

The Office of the Auditor-General's Forensic Audit Unit may have cause to conduct fraud or financial investigations in relation, but not limited, to the following types of misconduct:

- Procurement fraud
- Corruption and bribery
- Theft and embezzlement

- Financial Statement fraud
- Entitlements' fraud
- Misrepresentation
- Failure to comply with financial disclosure requirements
- Abuse of authority

There are various ways in which such fraud may be detected and includes the following sources of information:

- Whistleblowing
- Internal audit
- Internal tip off
- External tip off
- Fraud risk management, and
- Investigations by law enforcement agencies.

When an allegation of financial irregularity has to be investigated, a series of steps are necessary to decide whether fraud had occurred or not. In most cases of fraud, a tip-off (whistleblowing) begins the investigative process. Those with the intent and means to defraud a company or country will attempt to hide the crime. Forensic accounting investigators, highly knowledgeable and skilled in interviewing witnesses, collecting and analyzing evidence, writing reports, interacting with prosecutors in the courts, will be assigned the role of forensic investigators. These professionals, in the financial accounting field, are well trained to recognize the 'red flags' of improper financial practices and attempt to prove this by conducting a financial investigation. Because the investigation of fraud deals with the individual rights of others, the investigation must be done by an assigned investigator with sufficient cause or predication.

***Predication** is the totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud **has** occurred, **is** occurring, and/or **will** occur.*

Predication is the basis upon which an examination is commenced. Fraud examinations should not be conducted without proper predication. Any Investigation must be based on predication.

ACCOUNTING ANOMALIES (or Red Flags)

Accounting anomalies often signal the presence of financial fraud. Examples of accounting anomalies include:

- Account balances that are significantly over or understated
- Transactions not recorded in a complete or timely manner or improperly recorded as to amount, accounting period, classification, or organization policy
- Unsupported or unauthorized records, balances, or transactions
- Last minute client adjustments that significantly affect financial results (particularly those increasing income presented after submission of the proposed audit adjustments)
- Excessive number of adjusting entries, and repetitive use of adjusting entries for no apparent purpose.
- Conflicting or Missing Evidential Matter
- Suspicious or missing documents
- Unexplained items on reconciliations
- No original documents available – only photocopied documents
- Inconsistent, vague or implausible responses arising from inquiries or analytical procedures
- Unusual discrepancies between the client's records and confirmation replies
- Missing inventory or physical assets
- Excessive voids or credits
- Shifting of costs from one category or cost account to another
- Common names or addresses of payees or customers – inability to verify the existence of vendors/subcontractors
- Alterations on documents (e.g., back dating, white-out)
- Duplications (e.g., duplicate payments)
- Questionable handwriting on documents

These anomalies sometimes occur because there is a lack of (i) segregation of duties, (ii) physical safeguards, (iii) independent checks, and (iv) proper authorization or proper documents and records. Overriding of existing controls and an inadequate accounting system may also contribute to fraudulent practices.

PLANNING THE INVESTIGATION

The investigating of allegations of financial fraud with an intent to resolve, consist of two important features that determines the legitimacy and proper undertaking of a financial investigation: the investigating team and the investigative approach. The forensic accountant should engage a team comprising of individuals who has the required skills and knowledge to resolve the fraud allegation.

INVESTIGATIVE APPROACH

'Begin each case with the end in mind'.

This means to have a clear understanding, or picture, of the results of a successful fraud investigation. The success of an investigation can only be tested in a court of law, so it is critical to be able to clearly articulate results and findings in terms expected and accepted by the legal system. It will be left to lawyers and judges to decide what information is evidence and to judges and juries to decide the ultimate issue of guilt or innocence, or liability. Thus, the forensic professional must provide the required information upon which evidentiary and other legal decisions will be made. Preservation of evidence, party's rights, documentation of the processes and legitimate engagement of professionals must be ensured at all times for this to occur.

The information and evidence, developed through the application of the chosen investigative approach, must answer the following questions (5W's and the H) and be supported with the best and most comprehensive documentary evidence:

- a. When was the fraud committed?
- b. Who had the opportunity to commit fraudulent activity?
- c. What was taken (how much money was lost)?
- d. Where were the assets moved?
- e. Why was the activity intentional, rather than accidental, or the result of mistake or misunderstanding?

f. How were the assets converted to the benefit of the perpetrator?

THE FRAUD THEORY APPROACH

To solve fraud without support, the investigator must first make assumptions which the presenting evidence or what had occurred, indicate. Those assumption are tested to decide whether the fraud accusation is provable. Once tested and the allegations of fraud are not provable, the expert refines and retests the new theory/hypothesis which includes new evidence. This is done until allegations of fraud are proven or indicates that fraud had not occurred.

This approach to complex investigations is second nature to most investigators, at least the successful ones, but is misunderstood or neglected by others, with disastrous results. It is similar to the scientific method of experimentation, and involves the following steps:

- a. Analyze the available data to create a hypothesis;
- b. Test it against the available facts;
- c. Refine and amend it until reasonably certain conclusions can be drawn.

The approach begins with an informed assumption or guess, based on the available evidence, of what the investigator thinks may have happened, which is then used to generate an investigative plan to test – prove or disprove – the assumption. It is best illustrated by example:

Example of the Case Theory Approach

Investigator One receives anonymous allegations of corruption in the award of government contracts. He pursues the case with no case theory or investigative plan. He asks a dozen witnesses if they have any knowledge of payoffs; none do (this is not unusual). He subpoenas the contract files and whatever else he can think of but sees no smoking gun as he flips through them (this is even less unusual). He confronts the suspect, who denies any wrongdoing. The investigator does not know what else to do. He has assembled a thick file and an impressive command of the contracts but can prove nothing. Investigator Two pursues the same case, using the Case Theory approach:

- *He analyzes the available data – the details of the allegations.*

- *Creates a simple, initial hypothesis or theory, e.g., company A is paying kickbacks to government official B for government work.*
- *Makes assumptions which can be used to test the theory – e.g., if the allegations are true, official B would be expected to:*
 - *Favor Company A in buying decisions*
 - *Bend or break the rules to award contract to Company A*
 - *Display sudden new wealth or have unexplained income*

Investigator Two uses his hypothesis to organize the investigation, i.e., looks for evidence to confirm or rebut the theory (initially, this evidence is often the “red flags” of the suspected offense.)

The Case Theory approach generates the investigative plan (see if a, b or c occurred) and if the theory is correct, evidence of guilt. If not, the investigator may amend his theory, e.g., company C is paying official A, and try again. This approach also enables one to prove, to a certain extent, that a suspected act did not occur. Investigator One, after interviewing a dozen witnesses, did not know if bribes had been paid or not, only that he could not prove it. Investigator Two, however, can have some assurance that the alleged acts did not take place, if no evidence appears in support of his test assumptions. Remember, the Case Theory approach is simply an investigative tool to generate a hypothesis that can organize and direct an investigation, based on the information available at the time. It should not be treated as evidence itself. Do not be too committed to any particular theory and be ready to amend or abandon it as necessary.

TOOL USED IN FINANCIAL INVESTIGATION

There are three skills/tools in which a forensic investigator must be competent or well-equipped with, when conducting fraud investigations:

- a. Interviewing - the process of collecting information from those who have knowledge of the issue.
- b. Examination of financial statements, books and records - the forensic examiner must be aware of the law involved in obtaining and securing evidence. The Chain of Custody must also be maintained for documents and other important sources of evidence.

- c. Observing behaviours that would implicate persons involved in the crime. This often involves analysis of video surveillance footage.

Having the right financial investigative tools can determine the success or failure of an investigation.

INTERVIEWING

In terms of sequencing interviews are conducted after the forensic investigator analyses documents and concludes that the fraud theory is still applicable. They are an essential element of any investigation since oral statements can corroborate or clarify the information derived from documentary evidence, reveal new leads, or identify new financial documents. **(See Chapter 14 on Interviewing)**

Interviews of neutral third-party witnesses becomes the next step in an investigation.

- a. Neutral third-party witness – this is a person who is not involved in the specific instance of the fraudulent act.
- b. Corroborative witness – these witnesses are not associated with the specific offence but corroborate facts relating to the case.

CO-CONSPIRATORS

If after analyzing documents and both neutral and corroborative witness statements the examiner still determines that the fraud theory is applicable, the Investigator furthers his investigation by interviewing co-conspirators of the offence. Interview of co-conspirators is conducted from those that are least guilty to those that are most culpable.

TARGET

Interviewing the suspect or accused is conducted last even if he/she may not offer a confession. After all the facts are obtained, the examination of the suspect offers insight into the defence he/she may use or the information gathered may subsequently be used for impeachment.

INTERVIEWING NON-TARGETS

Important sources will be any complainants, the business associates, relatives, neighbors, employees, or other associates of the targets; business competitors, financial institution employees and other sources that have been in contact with the target.

DOCUMENT ANALYSIS

Three principles apply to analysis:

- a. It should be based on objective conclusions and not personal opinions.
- b. The source of evidence and information must be evaluated separately.
- c. It must be directly associated to the information

The following are used to analyze financial information:

- a. Comparative Statements – financial statements showing current financial position and profits for different periods.
- b. Trend analysis or pyramid method – Comparison of financial position over a series of years
- c. Ratio analysis or quantitative analysis – describes the noteworthy relationship which exists between items of a balance sheet and a profit and loss statement.
- d. Cash flow analysis – analyses the actual cash flow in a company
- e. Net Worth Analysis – to compare the received income on a financial statement with the costs that individual incurs.

Case Management

Developing effective and efficient strategies to make financial investigations an operational part of law enforcement efforts should be an imperative. Some investigations may be simple and straightforward, with witnesses and evidence readily available. However, serious corruption investigations, particularly those involving high-level or grand corruption, can be highly time-consuming, complex and expensive.

To ensure the efficient use of resources and successful outcomes, the investigative tools and personnel involved must be managed effectively. The work of the investigative team should be conducted in accordance with an agreed strategy and supervised by an investigative manager in charge of receiving information about the progress of

investigators regularly.

Key elements that will facilitate case management include:

- i. Periodically conducting needs assessments and promoting proper allocation of resources.
- ii. Articulating clear objectives for relevant departments and agencies that include effective coordinating structures and accountability.
- iii. Establishing strategic planning working groups to develop an effective policy that incorporates the skills of all relevant agencies into an action plan; these groups should include representatives from all relevant agencies and components participating in financial investigations.
- iv. Creating specialized investigative units focusing on financial investigations and asset tracing/freezing.

When managing a case, the sequencing of actions can be of the greatest importance. For instance, measures that pose a risk of disclosing to outsiders the existence of the investigation and, to some degree, its purpose (such as the interviewing of witnesses and the conducting of search and seizure operations) should not be undertaken until after other measures have been taken, as they will only be effective if the target has not been alerted. Besides, some procedures may become urgent if it appears that evidence could be destroyed, or illicit proceeds might be moved.

Investigative teams may be assigned to specific target individuals, or focus exclusively on particular aspects of the case in complex investigations. For example, one group might be engaged in the tracing of proceeds, while others interview witnesses or maintain suspects 'surveillance.

Chapter 2: Assembling an Investigation Team

Choose a Team Leader and Team Members

Assembling the team for an investigation is key for a successful outcome. There are key personnel that must be included to complete the case. There should always be a lead investigator who will direct the investigation. Their responsibilities include making sure the investigation has a schedule which is adhered to so that nothing is missed.

It is important that the team leader is competent in investigative techniques and analysis tools as he/she will be responsible for assigning duties to the team, act as a liaison between the team and management, and be responsible for reporting and briefing the Investigation Unit Head and Auditor-General on the findings.

Assembling the remainder of the team is equally important. The appointment of the right team will ensure that the investigation meets the set objectives and scope. It is crucial that no team member has supervisory control over any of the other team members or of the work involved so as not to compromise the investigation.

Each chosen team member should bring a specific skill set to the table with technical or operational experience that may be relevant to the nature of the investigation. In addition to experience, qualities that should be considered when choosing team members include integrity, objectivity, curiosity and perseverance, and openness to ideas.

The main role of the team is to collect facts, data, and any evidence, while establishing the sequence of events that led up to the event that caused the investigation. The team will analyze the information and develop its findings into conclusions. Once that is completed the team leader will complete a report for presentation to the Auditor-General.

When assembling the team consider bringing in outside consultants, who can offer expertise and objectivity that may be needed.

Things to Consider:

The following standards and principles should be considered and, as far as possible, adhered to during a fraud investigation irrespective of the size and composition of the Investigative Team.

- a. The purpose of the investigation is to examine and determine the **veracity of allegations** of corrupt or fraudulent practices and allegations of financial misconduct in relation to government assets and property.
- b. The Investigation Team shall maintain objectivity, impartiality and fairness throughout the investigative process and conduct its activities competently and with the highest levels of integrity. In particular, the Investigative Team shall perform its duties independently and shall be free from improper influence and fear of retaliation.
- c. The members of the Investigative Team shall immediately disclose any actual or potential conflicts of interest.
- d. Appropriate procedures shall be put in place to investigate allegations of misconduct on the part of any team member.
- e. The Investigative Team shall take reasonable measures to protect as confidential any non-public information associated with an investigation.
- f. Investigative findings shall be based on facts and related analysis which may include reasonable inferences.
- g. The Investigative Team shall make recommendations, as appropriate, to the Auditor General that are derived from its investigative findings.

Chapter 3: Investigatory Planning Checklist

When conducting an investigation, it is important to have a plan for the investigation. This plan should be followed so as to ensure that a sequence is followed from the commencement to the end. The investigation plan is also important to prevent missteps or mistakes.

The following Investigation plan can therefore be used on any investigation. If changes to the information in the plan are made during the course of your investigation, it can be recorded and adjusted accordingly.

THE INVESTIGATION PLAN TEMPLATE

Step 1 – The Investigation Overview

In this step the investigation team must consider the following

- a. The Issue to be investigated (the predication)
- b. How was the referral received?
- c. Was it a Referral? When was the referral received?
- d. When the case was accepted?
- e. Who is Investigator assigned to the case?
- f. Summary of the complaint (Understand the background)

Things To Consider: Risks to The Investigation

- a. Flight risk for suspects
- b. Destruction of documents
- c. Anticipated delays
- d. Lack of cooperation
- e. Fear of reprisal
- f. Collusion between witnesses
- g. Other risks

Involved Parties

- a. Complainant(s):
- b. Alleged wrongdoer(s):

- c. Witnesses:
- d. Other involved parties or agencies:

Step 2 – Scope of The Investigation

This step determining the scope of the investigation is key. The following therefore must be considered in the investigation plan.

- a. Sources of Evidence
- b. Documents needed
- c. Witnesses that will be needed
- d. Expert input for the case

Other Sources of Information to Consider

- a. The Employee handbook
- b. Applicable Law
- c. Company Policies
- d. Research Related to The Misconduct
- e. Areas Not Being Investigated and Why

Step 3 – Prepare the Investigation Steps

This step involves putting together the plan for the execution of the investigation. It details all activities.

The following is a suggested tracking sheet that should be used.

List of Activities to Be Performed

No	Activity	Person Responsible	Time Frame

Interview Plan with Locations

Interviews are a key part of any investigation as such an Interview plan should be developed (see Chapter 14 for conducting interviews).

No	Interview Subject	Location	Date and Time

Document Management

The management of the documents used in an investigation makes for a successful outcome for a case. It is very important that all documents used be logged and the vital ones that form part of the evidence of the case be protected.

The following must be considered for document management

- a. Where will documents be stored?
- b. How will documents be recorded?
- c. Who will have access to them?

Communication Plan

Having a communication plan involves the following;

- a. Who will have access to case information?
- b. Who will have specified access to certain information?
- c. Who will not have access to case information?
- d. Will law enforcement be involved?

Step 4: Costs and Budget

Planning for an investigation is very costly, therefore determining all cost and making a budget will be economical some of the cost that must be budgeted are as follows;

- a. Forensic Experts
- b. Travel And Related Costs

- c. Legal Advice
- d. Translation
- e. Transcription
- f. Administrative Cost
- g. E-Discovery

Timetable

A timetable can be used to monitor milestones so that the investigation can be completed on time and on budget. The following can be used to create a timetable

- a. Interviews completed
- b. Evidence gathered
- c. Investigation report

Step 5 – Confidentiality

To protect the integrity of the case, as well as evidence and witnesses, A high level of confidentiality must be maintained. These include from;

- a. Media:
- b. Other employees:
- c. General public:

Chapter 4: Using Case Management Software

Case management software is a digital system that enables companies to track and store information in a centralized location and report on their data. Case information is accessible to a variety of users so that stakeholders can collaborate on cases and share information in a secure environment.

A case management system can be installed on a local network or it can be web based. Web-based case management software is the most popular type, because it is available 24/7 and accessible from anywhere with an internet connection. Many companies purchase case management software to replace spreadsheet-based case incident and issue tracking systems that have limited features, inadequate security and no workflow support.

WHAT DOES IT DO?

A case management software system streamlines intake, case tracking and reporting. It consolidates all case information into a central repository to provide a single source of up-to-date information on ongoing cases. The most sophisticated case management software also provides a tool for reporting on all the accumulated data for risk management and prevention.

5 ELEMENTS OF A CASE MANAGEMENT SOFTWARE PLATFORM

There are five elements in a case management software system. These are;

1. Case Intake

A good case management system uses a variety of intake mechanisms for complaints or reports. The most basic of these intake mechanisms is an internal online form that presents users with the fields that need to be filled in. Other intake methods include a public-facing web form, telephone hotline, email inbox, SMS inbox, chat bot, suggestion/complaints drop box or even a designated person or office (such as an ombudsman) to receive information.

Case management software intake includes:

- Recording new cases using an intake form
- Automatic (or manual) creation of a new case file to store all documentation
- Integration with other systems to create cases and pull information into the case file

- Notifications that parties may be involved in other cases
- Assignment of cases to the responsible person

2. Case Management

Case management activities make up the bulk of the work done in a case management system. This part of the software provides case managers with the tools they need to:

- Record notes
- Set reminders and alerts
- Assign tasks
- Track deadlines
- Set appointments
- Send and receive email
- Attach files
- Request approvals
- Link cases that have common parties or issues
- Follow investigative best practices through a rules-based workflow

3. Reporting

A great case management system has a strong reporting mechanism for making sense of all the data collected during the case management phase of an investigation. Reporting is critical for visualizing trends, detecting hot spots and conducting risk management and prevention. A great reporting tool will allow users to:

- Create new reports quickly and easily
- Create drill-down reports to see deeper into the data
- Choose from a variety of different types of charts and graphs to suit what's being visualized
- Build personalized dashboards
- Export reports to PDF, Excel, txt, csv and MS Word
- Distribute reports automatically or on an ad-hoc basis via email

4. Workflow

A good case management system has workflow rules and alerts to ensure that due dates are met and to make it easy for investigators, managers and executives to quickly understand the status of cases. Alerts can be set to advise users of:

- New cases created
- Case assignment
- Upcoming due dates
- Overdue escalation notices
- Case inactivity
- Requests to review cases or steps in a case

5. Access and Controls

All good case management software systems incorporate access controls to ensure the security and confidentiality of case files. Access to case information can be restricted based on a variety of criteria:

- Role – investigator, manager, executive
- Department – HR, legal, corporate security, compliance, health and safety
- Geography – country, state, region
- Individual – information can be blocked from someone who is related to a case or with a conflict of interest

Case management software is a powerful tool for investigators and anyone else who manages cases in a team environment. Replacing a spreadsheet-based system with a case management tool provides the secure access, collaboration, reporting and risk management necessary to resolve cases faster and boost prevention.

Chapter 5: Choosing Investigative Methods and Techniques

Determining which investigative tools to use depends on a variety of factors, including the nature of the alleged violations and the available resources.

In the course of the investigation, it is a normal progression to go from investigative measures that do not alert the targets that they are under investigation – and may include research of public databases, collection of public information, informal interviews of potential witnesses that are not closely connected with the targets, etc. – to measures that, once taken, allow the investigators to secure both evidences and proceeds of the crime. In other words, investigators must first arm themselves with as much information as possible to both ensure that potential witnesses –and, where admissible, defendants- tell the truth, and also keep criminal proceeds from being dissipated because the investigation becomes public.

The following are some of the investigative techniques that maybe used;

a. Interviewing Witnesses and Defendants (see Chapter 14)

Conducting interviews is one of the techniques that investigators can use to gather evidence and information in furtherance of their investigation. Interviews with potential witnesses or suspects – for those countries where cooperation of suspects might be exchanged by leniency – however, should not commence before considering the potential negative impact on the investigation by soliciting the witness 's co-operation. Even if not required by the criminal procedure rules, detailed reports of investigation should be completed to document interview results. Interview reports may be helpful in refreshing investigators and witnesses 'recollections of events during criminal or civil formal legal proceedings.

Still, the investigator should by no means be satisfied with interviews as a sole piece of evidence during an investigation. Testimonies and facts recollected through informal interviews should be tested to be confirmed through all other legal means of obtaining evidence to overcome the presumption of innocence.

b. Physical Surveillance

This is a useful technique to gain general background and intelligence on individuals/businesses, habits and relationships of suspects. It may also include electronic surveillance, through the use of visual surveillance in public places with the use of photography, video recording, optical and radio devices. Surveillance can be especially useful in financial investigations in cases involving the movement of bulk currency and by identifying — gatekeepers involved in the development and implementation of especially money laundering schemes. Surveillance of targets can often identify where financial and related records might be stored and lead to the discovery of assets. In addition, surveillance can help corroborate financial data and identify other targets and associates.

c. Trash Runs

This consist of searching the suspect 's discarded trash for evidence. It can be an effective way of obtaining leads as to where assets are maintained, as well as help develop probable cause for more coercive measures and evidence for use at trial. Suspects frequently discard evidence, including financial records and correspondence that may be valuable to a financial investigation.

d. Searches and Other Compulsory Measures to Obtain Evidence

These measures should be used to gather evidence of criminal activity that cannot be obtained by other means without authorization from a competent authority. The timely use of these powers to obtain evidence minimizes the opportunity for suspects to purge records and/or destroy evidence. In addition to seizing paper documentation, investigators should intercept or seize information from computers and other electronic devices, such as telephone, fax, e-mail, mail, public or private networks. The execution of these powers should always be properly planned and be lawfully conducted in accordance with existing policies and procedures.

SPECIAL INVESTIGATIVE TECHNIQUES

Although investigators of corruption cases tend to rely heavily on basic investigative techniques, good practice shows that more focus should be given to the use of special investigative techniques, financial investigations and international cooperation for the

successful investigation and prosecution of complex and cross-border corruption crimes. Special investigative techniques are applied by competent judicial, prosecuting and investigating authorities in the context of criminal investigations for the purpose of detecting and investigating complex criminality, in order to gather information in such a way as not to alert the target persons.

Special investigative techniques, although effective, entail serious risks that should be adequately addressed. Countries should ensure: that their competent authorities are properly trained in using these techniques, that clear policy and procedural guidelines are established and followed, and that proper operational oversight is conducted at the managerial level.

The following techniques have proven useful in corruption and financial investigations;

a. Intercepting Communications

Electronic surveillance techniques, such as electronic intercepts of wire, oral communications, electronic media and the use of tracking devices, can be very useful in financial investigations. This technique can help identify co-conspirators, provide insight into the operations of the criminal organization, provide real time information/evidence that can be acted upon using other investigative techniques and can lead to the discovery of assets, financial records and other evidence. Competent authorities should be trained in these techniques in accordance with the basic principles of their domestic laws.

b. Controlled Delivery

This is an effective investigative technique involving the transportation of contraband, currency, or monetary instruments to suspected violators under the control of law enforcement officers. Cross-border controlled deliveries can be performed in cooperation with customs and other foreign competent authorities, or on the basis of international agreements. Controlled deliveries are conducted to:

- i. Disrupt and dismantle criminal organizations engaged in smuggling contraband, currency, or monetary instruments across borders.
- ii. Broaden the scope of an investigation, identify additional and higher-level violators, and obtain further evidence.

- iii. Establish evidentiary proof that the suspects were knowingly in possession of contraband or currency.
- iv. Identify the violator's assets for consideration in asset forfeiture proceedings.

c. Cross-Border Observation

This investigative technique allows keeping a person who is located in a foreign economy under observation, with the authorization of the competent authorities of such economy. It may be used to keep under observation a person to which extradition may apply, or a third person who will probably lead to the offender.

d. Undercover Operation

Undercover operations typically allow investigators access to key evidence that cannot be obtained through other means. An undercover operation is an investigative technique in which a law enforcement officer or a person cooperating with the competent authority, under the direction of a law enforcement authority, takes undercover action to gain evidence or information (e.g., by infiltration of an officer under false identity into a criminal group). This technique includes the use of undercover companies (i.e. the use of an enterprise or an organization created to disguise identity or affiliation of individuals, premises and vehicles of operative units), informants (i.e. voluntary confidential cooperation with individuals to obtain information about crimes being plotted or already committed; informants can operate openly or secretly, free of charge or for a fee, can be hired as permanent or non-permanent staff) and use of agents provocateur or integrity testing (i.e. an investigator or other agent acting undercover to entice or provoke another person to commit an illegal act).

Properly conducting undercover operations often requires substantial resources, extensive training and significant preparatory work. The resources it requires, the unique and diverse skill sets it demands and its inherent risks typically make this technique a last resort – normally after other investigative techniques have been unsuccessful. Various significant factors should be considered when envisaging an undercover operation, including the legal framework, whether positive results are actually likely to be achieved, and the reliability of the informants under use.

Given the inherent risk with this technique, undercover operations proposals should be reviewed and authorized by designated officials from the competent law enforcement authorities. These officials should be knowledgeable on all aspects of undercover operations. Moreover, the proposal should indicate that traditional investigative techniques have been utilized and have been largely unsuccessful and that the undercover operation is likely the only technique available to gather evidence of the suspected criminal activity. Only highly trained undercover agents should be used in undercover operations.

Undercover operations should be re-evaluated in an ongoing manner, and investigators should always be prepared for its termination. Termination criteria should be established in advance.

The actions performed by law enforcement during undercover operations should be in accordance with the basic principles of existing laws, policies and procedures, and all undercover officers should be highly trained before engaging in such operations.

Chapter 6: Investigating Corruption

Given the extent of corruption, the range of cases likely to exist, the variety of possible outcomes, and the limits imposed by human and financial resource constraints, most anticorruption law enforcement agencies will find it necessary to make priority choices as to the cases to pursue, and the outcomes to seek. In practice, it must be recognized that not every suspected case can be fully investigated and prosecuted.

Moreover, detecting corruption itself involves a key problem. Although not a victimless crime, many crimes of corruption, particularly bribery and trading in influence, are consensual crimes and therefore complainants are hard to find. Furthermore, as corrupt deals usually occur without witnesses, are rarely documented and are normally surrounded by secrecy, few overt occurrences are likely to be reported by witnesses, unless they are insiders. The importance of intelligence in the pro-active detection of corruption therefore stands out.

Even though it is usually delimited by law or by specific agency guidelines, prioritizing a corruption case involves the exercise of considerable discretion, so it can be managed carefully to ensure consistency, transparency and the credibility of both the decision-making process and its outcomes. A major element in this regard is the setting and, where appropriate, the publication of criteria for case selection (sometimes referred to as a prosecution policy paper). This document can help reassure those who make complaints, as well as the general public that a decision not to pursue a particular reported case is based on objective criteria and not on improper motives.

Case selection criteria should include the following:

a. The Seriousness and Prevalence of The Alleged Offense

Assuming that the fundamental objective of an anti-corruption strategy is to reduce overall corruption, priority may be given to cases that involve the most common forms of corruption. Where large numbers of individuals are involved, or structural practices are targeted, the case will often lead to proactive remedial outcomes such as the setting of new ethical standards or the training of public officials, general preventive policies with large-scale remedial capabilities. Alternatively, as overall expertise and knowledge are

gained and greater numbers of cases are dealt with, intelligence information can be gathered and assessed, constituting a useful tool for prioritizing cases on the grounds of their seriousness. Intelligence should therefore guide case selection decision making processes through the detection of overall corruption patterns and the identification of such cases which are causing the most social or economic harm.

b. Related Cases in The Past to Establish Precedent

Priority can be given to cases that raise social, political or legal issues the results of which can be applied to many future cases. Examples include dealing publicly with common conduct not hitherto perceived as being corrupt in order to change public perceptions, and cases that test the scope of criminal corruption offences so that they either set a useful legal precedent or establish the need for legislation to close a legal gap.

c. The Viability or Probability of a Satisfactory Outcome

Cases may be downgraded or deferred if an initial review establishes that no satisfactory outcome can be achieved. Examples include cases in which the only desirable outcome is a criminal prosecution although it may not be possible or in the public interest to prosecute (i.e., the suspect has died or disappeared, is already serving a lengthy term in prison, is extremely old or critically ill) or where essential evidence has been lost. The assessment of such cases should include a review of whether other appropriate remedies may be available.

d. The Availability of Financial, Human, and/or Technical Resources to Adequately Investigate and Prosecute

The overall availability of resources is always a concern in determining how many cases can be dealt with at the same time or within a given time period. An assessment of costs and benefits before decisions are made is thus important. In cases of grand corruption and with transnational implications there can be substantial costs in areas such as travel and foreign legal services, but the public interest may demand that examples are made of corrupt senior officials for reasons of deterrence and credibility, to recover large proceeds hidden either at home or abroad and to restore faith in government.

A periodic reassessment of caseloads is required, since the burden of particular cases

tends to fluctuate as investigations proceed. A single major case, if pursued, may result in the effective deferral of large numbers of minor cases, and the unavailability of specialist expertise may make specific cases temporarily impossible to pursue.

e. The Legal Nature of The Alleged Corrupt Activity

Corruption can give place to either criminal or administrative/civil procedures. The nature of the offence will often determine which agency is competent to deal with it. The possibility of initiating action other than a prosecution, if circumstances allow, should be considered taking into account the criteria referred to here and the prosecution agencies' workload, among other factors.

Managing Transnational or Grand Corruption Cases

Cases involving "grand corruption" or that have significant transnational aspects raise especial management issues. For example, cases where high level officials are suspected raise exceptional concerns about integrity and security and are likely to attract extensive media attention. Large-scale and sophisticated corruption is well resourced and well connected; making it more likely that conventional sources of information will either not have the necessary information or evidence or be afraid to cooperate. Senior officials may be in a position to interfere with investigations. The magnitude of proceeds in grand corruption cases makes it more likely that part of the overall case strategy is the tracing and forfeiture of the proceeds, and where they have been transferred abroad, obtaining their return. Allegations that senior officials are corrupt may also be extremely damaging in personal and political terms if they become public and later turn out to be unsubstantiated or false.

Transnational elements are more likely to arise in grand corruption cases. Senior officials realize that there is no domestic shelter for the proceeds while they are in office and generally transfer very large sums abroad, where they are invested or concealed. In many cases, the corruption itself has foreign elements, such as the bribery of officials by foreign companies seeking Government contracts or the avoidance of costly domestic legal standards in areas such as employment or environmental protection. The offenders themselves also often maintain foreign residences and flee there once an investigation becomes apparent.

Generally, transnational, or multinational investigations require much the same coordination as do major domestic cases, but the coordination and management must be accomplished by various law enforcement agencies that report to sovereign Governments which have a potentially wide range of political and criminal justice agendas.

Coordination will usually involve liaison between officials at more senior levels and their foreign counterparts to set overall priorities and agendas, and more direct cooperation among investigators within the criteria set out for them. From a substantive standpoint, investigative teams in such cases will generally be much larger and will involve additional areas of specialization such as extradition, mutual legal assistance and international money laundering.

Identifying Potential Targets

Embezzlement of public funds and corruption cases always involve personal gains. From the criminal perspective, an important part of keeping the crime uncovered is to bring satisfactory benefits for all those included in the scheme, in order to ensure their commitment to secrecy. Therefore, in order to identify potential targets of the investigation it is important to follow the money or other forms of gain or benefits, and determine who profited from the corrupt act and how. To such end, the following suggestions should be taken into account:

- i. Tax returns, financial disclosure forms, employment records, and loan applications should be reviewed;
- ii. Immediate superiors and fellow employees are usually good sources of information (suspects have a way of revealing themselves and their processes to those they associate with on a daily basis);
- iii. Public registries, credit card accounts, expensive celebrations, school fees and support measures for children, foreign bank accounts, homes and second houses and holiday homes should be located and assessed, as well as means of transport and employees' salaries and perks;
- iv. Even at these preliminary stages, experts should be on hand for consultation, even in an informal fashion. Document examiners, for example, can be consulted for

handwriting examinations, signatures, paper and ink analysis and comparison, erasures or substitution of documents, and restoration of obliterated writing. Fingerprint experts, experts in computers and cybercrimes (e-commerce fraud, stenography analysis, data recovery, etc.) and experts in DNA testing (for intimate contact items, such as used stamps and envelopes) may be of great help.

- v. Once a particular suspect has been identified (or grounds for suspicions arise), the screening process should include persons with whom they have strong ties (family members, business associates, etc.) considering that bank accounts, real estate, land or stocks are often in the names of people of the suspect 's trust.

Chapter 7: Building Coordination and Cooperation Networks

More often, it is necessary to resort to counterparts in other agencies, such as tax agencies, customs, financial intelligence units (FIUs), supervisors of the banking, insurance and securities sectors, public procurement agencies, etc. Liaising with such agencies is usually subjected to both legal and practical challenges of coordination and cooperation.

This chapter captures some best practices used in order to overcome these challenges, in particular when engaging with FIUs at the domestic level (Section B) and with foreign counterparts of a different nature (Section C).

Internal Cooperation and Coordination

The creation of institutional conditions that ensure that investigative specialized units can work closely with different competent enforcement authorities is fundamental for successful investigations. For example, information from tax authorities, oversight institutions, or FIUs can help tracing assets that may have been derived from corruption. Mechanisms that have been stressed for the promotion of intra and inter-agency cooperation include;

- a. Establishing information sharing systems whereby all investigative services would be aware of previous or on-going investigations made on the same persons and/or legal entities so as to avoid replication.
- b. Establishing policies and procedures that promote the sharing of information/intelligence within intra-agency and inter-agency cooperative frameworks; such policies and procedures should promote the strategic sharing of the necessary information.
- c. Establishing a process whereby intra-agency or inter-agency disputes are resolved in the best interest of the investigation.
- d. Establishing written agreements such as Memorandums of Understanding (MoUs) between agencies to formalize these processes.

Given the need for autonomy and independence on the part of investigators, and taking into account the extreme sensitivity of many corruption cases, care must always be taken when establishing relationships between anticorruption bodies and other government agencies (e.g., internal inspection and audit within government agencies), especially in environments where corruption is believed to be widespread.

Multi-Disciplinary Groups or Task Forces

SOURCE: FATF Report. *Operational Issues. Financial Investigations Guidance*, June 2012, p. 17-19

Particularly in large and complex financial investigations, it is important to assemble a multidisciplinary group or task force to ensure the effective handling of the investigation, prosecution and eventual confiscation. There should be a strategic approach to intra-agency and inter-agency cooperation in an effort to support information/intelligence sharing within and between agencies and with foreign counterparts.

Multi-disciplinary groups or task forces serve to integrate information from different law enforcement and intelligence sources, which had previously been separated by organizational and technical boundaries. In some jurisdictions this requires changes in laws and regulations or may require formalized agreements such as Memorandums of Understanding (MoUs). These task forces leverage existing technologies and develop new technologies in order to provide cross-agency integration and analysis of various forms of data. Furthermore, this information is stored in centralized databases so that any future investigation of any new target of a participating task-force agency can be cross-referenced against that historical data.

Multi-disciplinary groups may comprise a range of individuals, including specialized financial investigators, experts in financial analysis, forensic accountants, forensic computer specialists, prosecutors, and asset managers. Experts may be appointed or seconded from other agencies, such as a regulatory authority, the FIU, a tax authority, an auditing agency, the office of an inspector general, or even drawn from the private sector on an as-needed basis. The multi-disciplinary groups should include individuals with the expertise necessary to analyze significant volumes of financial, banking,

business and accounting documents, including wire transfers, financial statements and tax or customs records. They should also include investigators with experience in gathering business and financial intelligence, identifying complex illegal schemes, following the money trail and using such investigative techniques as undercover.

operations, intercepting communications, accessing computer systems, and controlled delivery. Multi-disciplinary groups should also consist of criminal investigators who have the necessary knowledge and experience in effectively using traditional investigative techniques. Prosecutors also require similar expertise and experience to effectively present the case in court.

Collaboration between Law Enforcement Agencies and the AOG

The AOG, the FIU and other law enforcement authorities should seek, ***where legally permissible***, to work together as a team by sharing information in appropriate circumstances to support financial investigations. This, of course, will depend upon each authority's capacity to share information, the extent, what and with whom it may be lawfully shared. For example, providing an FIU with an information requirement – detailing information priorities – may assist the FIU in identifying useful information for spontaneous dissemination to the AOG. Many investigative authorities have seconded personnel working in the FIU, or FIU personnel seconded to investigative authorities to facilitate cooperation and information exchange. Single points of contact in between investigative authorities can also assist consistent, and efficient information exchange.

Documenting how competent investigative authorities and establishing communication channels can provide clarity on the procedures and processes that are required in order to exchange information appropriately. Formal arrangements between investigative authorities can be documented in Memoranda of Understanding/Agreement (MoUs) and standard operating procedures (SOPs). Agreeing on the use of standard electronic reports and request forms that can be securely exchanged between investigative authorities can also facilitate efficient exchange of information. When exchanging bulk or structured data in relation to financial investigations (such as computer files with analysis results) consideration should also be given to the compatibility of the software used by competent authorities.

Use of FIU's Intelligence as Evidence

Financial disclosures and FIU analysis are usually considered a particular category of information. As stated, they constitute a particularly valuable source of information to law enforcement and, particularly, financial investigators. Given that the main focus is on the use of STRs, the unique nature of this data should be highlighted.

STRs information is mostly used for intelligence purposes and is not directly used as evidence in court proceedings. Intelligence information obtained through FIUs usually need to be re-obtained through Court proceedings. The rationale behind this principle is that the restrictions of individual rights – sometimes privacy, sometimes property - which might follow the introduction of such information into a legal proceeding are subject to Court authorization.

In addition, and for the same reasons, there are also strict confidentiality rules associated with access to and use of this information. It is essential that only competent and appropriately trained law enforcement officers have access to this information.

Chapter 8: What is Evidence

Evidence is a tool by which innocence or guilt is proven in a justice system. It is used to find the facts and is presented in court based on its admissibility. As Forensic Accounting Practitioners and fraud investigators, evidence is an integral aspect of any enquiry and it is sometimes disheartening to prepare and present an investigative report in which parts may be considered “inadmissible”. It is therefore essential that the forensic expert knows how to gather, secure and ensure the admissibility of evidence in any investigation. Evidence is admissible in litigation proceedings as proof of an issue/matter. It is important to maintain proper management of the evidence so as to extract it without tampering or altering it. Evidence management must also maintain accountability of evidence when it is passed from person to person for analysis, evidence from technological devices must be especially carefully secured to avoid loss of important information intended for evidence.

The Basic Rules of Evidence is a system of rules and standards that is used to determine which facts may be admitted as evidence, and to what extent a judge or jury may consider those facts, as proof of a particular issue in a lawsuit. The main goal of evidence collection in any forensic investigation therefore, is to ensure its admissibility in any legal proceeding.

The Rules of Evidence

To be admissible as evidence in a legal proceeding, a document or other material must be authenticated or identified as to what its proponent claims it to be. The Rules of Evidence outlines the rules for admitting evidence and the weight the evidence holds in any trial/case. The basic prerequisites of admissibility of evidence are relevance, materiality, and competence.

In general, if evidence is shown to be relevant, material, and competent, and is not barred by an exclusionary rule, it is admissible and can be used as probative of an issue. These Rules of Evidence is applied, it ensures fairness in administration, avoids delay and additional costs in litigations and promotes the use and improvement of the laws of evidence so that the truth in any proceeding is always justly determined.

What is Relevance, Materiality and Competence?

- I. Relevant evidence is evidence that is admissible in court based on the fact that it directly pertains to proving the case at hand.
- II. Materiality is a description of the quality of evidence that possesses such considerable probative value as to establish the truth or falsity of a point in issue in a lawsuit. The evidence in essence must be persuasive.
- III. Competency refers to evidence that is appropriate and needed to prove the issue of fact that the parties have made. Competent evidence may also serve as a link to the subject matter that is to be proved.

Types of Evidence

Evidence is divided into four (4) main types:

- I. **Demonstrative Evidence** – this is evidence that illustrates testimony: replicas, charts, diagrams, photographs, that is usually presented by qualified experts. Demonstrative evidence has no probative value when presented by itself. The forensic expert will be instructed to calculate and analyze findings and prepare exhibits for presentation in litigation proceedings. In order to be presented as evidence, the exhibits must be relevant to the issue at matter. The judge reserves the right to not admit demonstrative evidence if he/she finds it to be prejudicial or inappropriate, or if it's distorting or confusing. The prepared exhibits must be specific when prepared for presentation. If mistakes are identified by the opposing attorney, the credibility of the expert is questioned and the probative value of the evidence submitted is decreased.
- II. **Documentary Evidence** – this is any document whether written , printed or recorded material, which is presented and allowed as evidence in a trial or hearing, as distinguished from oral testimony, to establish the existence or nonexistence of a fact that is in dispute. It may include business records such as sales receipts, inventory lists, invoices, bank records, including checks and deposit slips; insurance policies; personal items such as diaries, calendars, telephone records, any law enforcement agency reports including investigation reports, department dispatcher logs, written transcripts of audio or videotape recordings, a map, plan, graph or drawing, a

photograph, disk, tape, soundtrack or other device in which sounds or other data (not being visual images) are stored. Business's financial records, job acquisition documents, meeting notes, plans, proposals and projections documents, statistical analyses, notebooks of stenographers, summaries, tabulations, telegrams and messages are all considered documentary evidence. Documentary evidence is generally admissible if the documents or items are maintained in the normal course of business.

III. **Testimonial Evidence** – covers what witnesses say under oath or affirmation.

IV. **Real Evidence** – includes all types of tangible objects

The Chain of Custody

The Chain of Custody is of utmost importance and must be maintained for documents and all other important sources of evidence. The Chain of Custody refers to the documentation that establishes a record of the control, transfer, and management of evidence. In other words, preserving the chain of custody means always being able to account for the safekeeping of all original evidence after it has been secured, including keeping a full record of its movement and the signatures of all persons to whom the evidence has been transferred. For this purpose, all items of evidence should be individually numbered and descriptively labelled. For example, to prove someone guilty, a prosecutor must prove that the evidence presented in court is the same evidence that was recovered at the scene of an alleged crime.

Chapter 9: The Gathering of Information and Evidence

Prosecuting and proving a crime is often much more difficult than investigating and solving it. Due to the dire consequences of a criminal conviction for the fundamental rights of the convicted person, criminal cases have a stricter burden of proof than civil cases. To overcome the presumption of innocence and for a person to be convicted, that person must be proved guilty beyond any reasonable doubt.

Thus, the gathering of credible information and evidence that supports the commission of a crime is often essential in the early stage of an investigation, since it allows law enforcement agencies to move forward by securing warrants for search, seizure, or intercepting phone calls and e-mails. However, the AOG's Forensic investigators can rely on powers granted by Sections 30 to 34 of the Audit Act to undertake searches, seizures etc. of any relevant national, local or regional government offices or agencies. But may require the assistance of a law enforcement authority where the desired information is not secured in any of the aforementioned locations.

In order to be admissible, evidence must be obtained in accordance with the applicable criminal (or civil) procedure rules as well as the constitutional rights of the defendants or any other affected third party. The fact that unlawfully obtained evidence could be declared inadmissible in court and therefore jeopardize the success of the prosecution or confiscation, all evidence should be legally obtained and, accordingly, law enforcement agencies should be familiar with the legal framework applicable to the evidence collection process. Legal experts' advice should always be sought by agencies in dealing with the gathering of evidence.

Once evidence has been legally collected, it should be subject to an assessment in order to review the progress of the investigation and explore whether any additional line of inquiry can be identified. Investigators are advised to follow a standard model of evaluation like the one shown in the following flow figure since it will allow them to evaluate the collected material in a consistent, structured, and auditable way.

The Evidence Evaluation Flow

1. Setting The Objective of The Evaluation

In the early stages of an investigation, the objectives are likely to be broad and concerned with whether a crime has been committed, whether a suspect and witnesses can be identified, what material can be gathered, etc.

As the investigation progresses and initial ends are achieved, the objectives will narrow. They will vary depending on the crime, the available material and the stage of the investigation. The evaluation process should be sufficiently flexible to accommodate such changes.

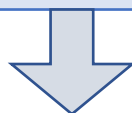


2. Evidential Filters

Relevance – Whether gathered materials have some bearing on any offence or person under investigation, or on the surrounding circumstances of the case, must be evaluated

Reliability – The reliability of materials should be reviewed during the evaluation process to ensure that any potential problems have not been overlooked. Investigators should have a clear understanding of the impact the reliability of material may have on the investigation and the strength of the prosecution case. An element can have high reliability if it can be corroborated by an independent source, and less reliability if it cannot be corroborated and conflicts itself with other materials gathered in the investigation.

Admissibility – This test should ensure the investigators that the gathered materials will be available to the courts in an evidentially acceptable format. Investigators must be aware of the legal framework and must seek legal advice on what constitutes an acceptable evidential format in relation to any material.



3. Organizing Knowledge

In the first instance the objective of an investigation is likely to be broad and concerned with establishing what information there is, what type of incident is being investigated, whether or not a crime has been committed and if there is a suspect.

The 5WH formula (Who – What – When – Where – Why – How) has been found to be a highly effective way for investigators to organize their knowledge in the early stages of an investigation. When gathering evidence, the investigator must ask;

- a. Who are the victim(s), witnesses, and suspect(s)?
- b. Where did the offence take place?
- c. What has occurred?
- d. When did the offence and other significant events take place?
- e. Why was this offence committed?
- f. How was the offence committed? Assess the use of skills or knowledge used by the offender.

Subsequent evaluations will replace the broad objectives with more specific objectives. The way in which investigators then choose to organize their knowledge will change to match these more specific objectives.



4. Testing Interpretation

There are a number of ways in which investigators can test the validity of their interpretations of the gathered material.

Self-review: Investigators should thoroughly check their work and review any assumptions they have made during the evaluation process.

Peer Review: Checks by supervisors or colleagues provide a second opinion on the interpretation of material.

Expert Review: Where investigators use material produced by experts such as forensic scientists, they should consult the expert to ensure that the outcome of the evaluation is consistent.

Formal Review: In complex cases a formal review of the investigation can be carried out by a suitably qualified officer.

SOURCES OF INFORMATION

As already indicated a variety of sources can be relevant to financial investigations, including interviews, searches, forensic examination of computer(s), collection and analysis of financial and business records, tax authorities 'reports, etc.

There are several ways to categorize potential data sources. The Inter American Drug Abuse Control Commission of the OAS (CICAD) has proposed a classification of sources of information that is also applicable to corruption investigations which OAG investigators may find useful:

Patrimonial Sources of information related to asset ownership of an individual or company (vehicles, real estate, horses, jewels, industrial real estate, airplanes, stocks, weapons, etc.)
Legal Sources of information related to civil, criminal, business, and labor litigation of an individual or company.
Business Sources of information related to economic activity or business conducted by an individual or company.
Police Sources of information related to traffic infractions, fines, or any other relevant police information.
Corporate Sources of information related to incorporation of companies and changes in partnership quota, trust funds, board of directors, etc.
Normative Sources of information related to an economy's norms and regulations, and its jurisprudence.

Financial Information

Information about the financial affairs of relevant organizations help to understand their nature, resources, structure and capabilities, and helps predict future activity and locate assets. This information is normally maintained by private parties, including bank accounts, financial accounts, other records of personal or business financial transactions and information collected in the context of meeting customer due diligence (CDD) obligations.

Financial Institutions

Financial institutions not only holds information about the movements of a bank account, but also about direct debits, standing orders, credit and debit slips, supplemental information such as managers' written notes, account opening forms, copy of identification used to open the accounts, safety deposit boxes, copies of ledgers of business, credit and charge card accounts, credit and charge card statements, pensions, insurance schemes, mortgages and even other previously unidentified accounts.

Requesting Financial Information from Financial Institutions

The importance of gathering information available through public opened sources is that such information is usually only the basis for requesting access to information held by financial institutions. This information includes, but it is not limited to:

- Bank accounts
- All account-opening documentation, such as forms that identify the beneficial owner, partnership agreements, and copies of identity documents (not only accounts under the names of the targets, but also those accounts that list any of the targets as a power of attorney or a signatory)
- Bank account statements
- Credit and charge card accounts information
- Credit and charge card statements
- Standing orders
- Documents related to account transactions, including client orders, deposit and withdrawal slips, credit and debit memos, and checks

- Wire transfer documentation
- Managers' written notes, client profile, any due diligence conducted by the financial institution, any other data probing the economic background of the client
- Safety deposit boxes information
- Copies of ledgers of business
- Pensions and insurance schemes
- Mortgages and loan documentation
- Other previously unidentified accounts
- Any reports of suspicious activity that were submitted by an employee of the financial institution
- Correspondence files maintained by the financial institution

The information contained in these documents can show the lifestyle of a person, his/her spending patterns (i.e., their travels, meals, vacations, hobbies or other interests) and whether a person is living beyond their means or has any financial problem.

In addition, automated teller machines (ATM) can provide information on:

- Sums withdrawn
- Geographical location at a certain time
- Routines.

This information will almost certainly be considered protected by the right to privacy. Therefore, accessing to such information is subjected to specific standards of evidence showing that, *prima facie*, the information may be used as evidence in a criminal case.

In addition to requesting production orders to access information held by the regulated sector or service providers, investigators may need to monitor the transactions of a specific financial product for a period of time. In such instances, some jurisdictions allow for the request to -account monitoring orders^{ll}, which are *ex parte* orders issued by a court requiring a particular financial institution to provide transactional information for a specific period of time.

Moreover, investigators may use customer information orders which include:

- The Account Number(s)
- The Person's Full Name
- Date of Birth
- Most recent address and any previous addresses
- Date(s) of account opening and/or closing
- Evidence of identity obtained by the financial institution for the purpose of money
- Laundering regulations
- Personal details (name, date of birth, addresses) of joint account holders
- Account numbers of any other accounts to which the individual is signatory and details of the account holders.

Customer's information on companies may also be useful, including details such as the value added tax identification number (VAT number), registered offices and personal details of individual account signatories.

In some jurisdictions, *credit reference agencies* provide, or similar private agencies provide information on an individual's financial relationships and status. The information provided by these agencies includes:

- Financial history and credit status, repossessions
- Names of financial associates
- Address checking
- Electoral roll data
- Insurance information
- Cars, purchases (hire purchase information)
- Properties
- County court judgments
- Telephone numbers and a list of all credit searches that have been carried out on a person including identity verifications
- Relevant information on fraud linked to a particular address, and details on repossessions

- Information on business proprietors (including cross-reference business registrations using address and telephone number data, and directors' names)

Legal Issues

SOURCE: StAR (Stolen Asset Recovery) Initiative, Barriers to Asset Recovery, 2011, pp. 58- 59, available at: <http://www.unodc.org/unodc/en/corruption/StAR.html>

Banking Secrecy Laws

Banks and other financial institutions in most jurisdictions are prohibited from divulging personal and account information about their customers except in certain situations mandated by law or regulation. Some jurisdictions deal with banking secrecy by giving prosecutors the ability to obtain information about the existence of an account but requiring that the prosecutor seek a judicial order to obtain additional information about the contents and transactions of the account. In some jurisdictions, a bank cannot divulge any information to a prosecutor about a bank account without judicial approval. It may even be a serious offense to provide information about a bank customer to any third party, including domestic or foreign governments, unless very specific criteria are met. Investigators have few alternatives to obtain information about specific accounts holding stolen assets where strict banking secrecy laws are in place.

Banking secrecy laws can also prevent law enforcement agencies from sharing banking information and documents with their foreign counterparts, even where these agencies wish to assist the foreign jurisdiction. To overcome this obstacle, the information is sometimes provided without a formal MLA request. For example, FIUs can obtain information on an FIU-to-FIU basis, and membership in Egmont Group of Financial Intelligence Units helps facilitate this cooperation and expedites the exchange by offering members access to the Egmont secure Web site. Information provided in this manner, however, is often not admissible as evidence in court. This restriction can mean that the authorities know where the proceeds of corruption are located but are unable to prove it in court and therefore are unable to restrain, seize, or confiscate the assets.

As stated in the Legislative guide for the implementation of the UNCAC:

Bank secrecy rules have often been found to be a major hurdle in the investigation and

prosecution of serious crimes with financial aspects. As a result, several initiatives have sought to establish the principle that bank secrecy cannot be used as grounds for refusing to implement certain provisions of international and bilateral agreements or refusing to provide mutual legal assistance to requesting States. The same applies to the Convention against Corruption, as we have seen above with respect to seizure and confiscation of proceeds of crime (art. 31, para. 7; see also para. 8 of art 46 (Mutual legal assistance)).

In cases of domestic criminal investigations of offences established in accordance with the UNCAC, State Parties are required to ensure that their legal system has appropriate mechanisms to overcome obstacles arising out of bank secrecy laws (Article 40). In accordance with Article 31, State Parties must – to the greatest extent possible under their domestic system – have the necessary legal framework to enable, inter alia, the empowerment of courts or other appropriate authorities to order that bank, financial or commercial records (such as real estate transactions, shipping lines, freight forwarders and insurers) be made available or seized. Bank secrecy should not be a legitimate reason for failure to comply.

Legal Privilege

A barrier similar to bank secrecy laws may arise where claims of lawyer-client privilege prevent investigators from looking at transactions involving lawyers. Legal privilege is an important right and should be recognized in all jurisdictions. The privilege should not apply, however, in cases where the lawyer is providing financial services, rather than legal advice, or is acting as a financial intermediary.

Financial information is usually crossed with databases and registers (i.e., registers of companies, data of stock exchanges), disclosure forms (asset disclosures, financial and tax statements by public officials and other persons) and available information about salaries, income and spending (bills, expense reports). In a financial investigation, it is essential to conduct a thorough and combined analysis of these documents.

Credit Reference Databases

Credit reference agencies provide data access systems that can be used in criminal

investigations allowing authorized officers to obtain information on an individual's financial relationships and status. This information can assist in the prevention or detection of crime and apprehension and prosecution of offenders, or the assessment or collection of any tax or duty.

Regulatory Information

Information that is maintained by regulatory agencies; access is typically restricted to official use only. This category of information could be held by central banks, tax authorities, other revenue collecting agencies, registry agencies, etc.

Gathering Peripheral Evidence

At the preliminary stage of any investigation, law enforcement agencies should rapidly gather information from all available sources. Data collected in this phase can therefore provide the factual basis to bring the investigation to the next stage, which might involve the need for a judicial warrant to be applied for before the competent authority. Because the data collected might be filed in a judicial proceeding, the acquisition process is a sensitive moment.

At this stage, immediately available sources are in particular the so-called open sources and government agencies databases (publicly and not-publicly available). Those are typically referred to as the source of first resort, because every information collector should exploit them as the first step in the information-collection process.

Open Sources Evidence – General Aspects

Open-source information has been defined as publicly available information that anyone can lawfully obtain by request, purchase, or observation. The use of open sources techniques is a rising area of intelligence gathering. As the public globally embraced the World Wide Web in the mid-to-late 1990s, the internet emerged as the primary source for search for all types of information. In the so-called -information age, the Internet provides access to a huge amount of significant, updated information, which has proven to be of dramatic importance for law enforcement agencies. Investigators must ensure that the information collected from open sources is accurate and reliable. The challenge, particularly when massive amounts of

information are available, is to make good end user decisions about what information should be kept and which information should be discarded.

Open sources can be used for a variety of purposes. One of the most common uses is to identify and verify a wide range of facts: personal identity information, addresses and phone numbers, e-mail addresses, vehicles known to have been used, property records, are among a wide variety of other facts that can easily be identified through open-source public and commercial databases and directories. Open sources can also help in understanding the motivation or rationale of individuals involved in criminal behavior, it can especially be useful in corruption and money laundering investigation, as well as in the process of recovering stolen assets.

Open sources intelligence includes methods of finding, selecting and acquiring from publicly available sources, and analyzing such information to produce credible intelligence. Open source is distinguished from research in that it applies the process of intelligence to turning hard data and information into intelligence to support strategic and operational decisions.

Open-source intelligence requires a certain degree of specialization. Thus, the effective use of the internet to gather information is a specialized area of work, and secure methods of searching must be employed so as not to compromise operations. Intelligence in this sector requires different skills, such as the ability to analyze aggregate information. Information obtained from open sources tends to fall into two categories, namely one involving information about individuals, and, secondly, involving aggregate information. The aggregate information available is extensive which is where the skills of a qualified analyst come into play as it is a real challenge to assess what is reliable and what is relevant for the purposes of constructing intelligence.

Legal Issues

From a law enforcement perspective, one of the values of open-source information is that it can be usually searched for and collected without a legal process. However, it can raise important legal issues, i.e., civil rights issues related to the retention of open-source information for the intelligence process.

AOG investigators must be vigilant in the managing of open-source information because of the regulatory framework that might apply to information retention in a criminal intelligence records system. When information is being gathered via open source and is being retained as intelligence, human and constitutional rights claims may arise.

Open source can lead to the mining of important and sensitive information about an individual, for example, a person's credit rating. Therefore, once the information is retained and forms part of an intelligence assessment and a file, questions and processes need to be carefully considered to ensure compliance with the broader issues under human and constitutional rights. The key is not the source of the information but what is being retained and how it is being retained.

Information About Individuals and Organizations

As a general rule, when a law enforcement agency conducts an open-source search for information, the agency should assume that civil rights protections attach to any information that identifies individuals or organizations, no matter how innocuous that individual piece of information appears to be.

Aggregate Non-Identifying Information

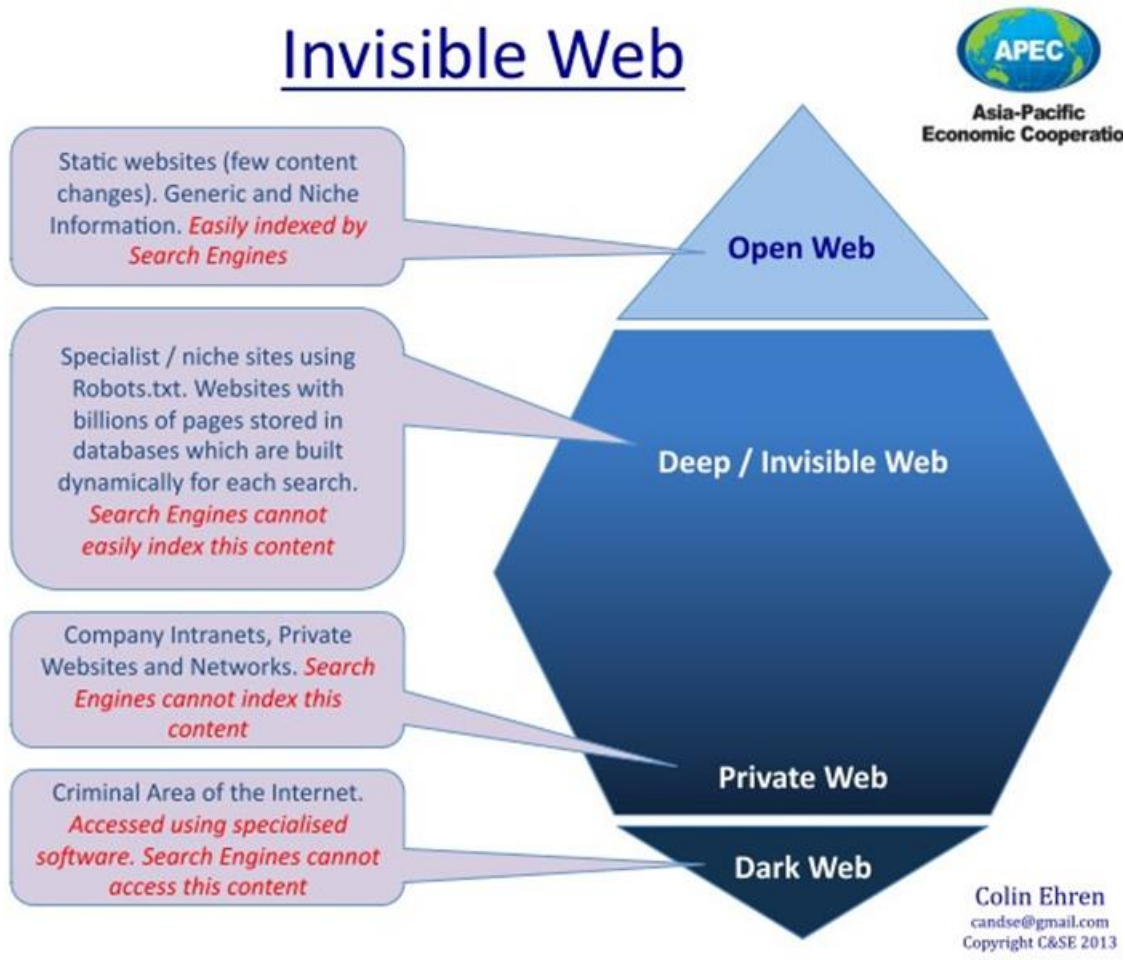
As a general rule, usually no civil rights attach to aggregate information or descriptions of issues, trends, ideologies, and so forth that does not identify an individual or organization.

Open Sources Evidence – Search Engines and the Deep, or Invisible Web

Currently, hundreds of search engines are available to retrieve information from the internet. However, they can easily index only the Open web, i.e., static websites, with generic and niche information. Search Engines cannot easily index this content, but that does not mean that deep web is not searchable. Investigators must rely on tools that can locate valuable open-source deep web information.

The most effective ways to search the deep web is to use search utilities that are designed to explore specific databases. While this still reaches only a portion of the deep web, the information gained from these databases can be extremely valuable. Deep web searching of databases typically requires accessing a variety of web sites to search for the desired information.

What should be apparent is that much of the deep web is not hidden in a surreptitious manner. Rather, it is hidden because it contains information in formats or architectures that are not readily identifiable by standard search engine technologies. As a result, it takes specially designed search utilities and greater effort by the user to identify and capture deep web information.



Open Sources Evidence – Social Media

Social media has become a useful tool used in an investigation. Agencies may use social media as an investigative tool when seeking evidence or information about a wide range of criminal activities. Social networking sites provide a multitude of information about individuals and persons with whom they interact. Social media sites contain identity information of the user and his or her contacts, often with photographs, as well as private messages and statements about beliefs and behavior. While some information, such as a private message,

is subject to legal process, a great deal of information is available as an open source.

Examples of social media include;

- Blogs
- Social networking sites (LinkedIn, Facebook, Instagram, Twitter, YouTube,)
- Microblogging sites
- Photo- and video-sharing sites,
- Location-based networks
- Wikis
- Mashups
- RSS feeds
- Podcasts

Social Media Monitoring Tools

Law enforcement agencies can rely on social media monitoring tools to capture data and monitor social media sites. These tools offer the ability to search for keywords and thus enable law enforcement to aggregate large amounts of data and refine them into smaller items of interest. Examples of these are, Twitterfall, Netbase, Trackur, CrowdControlHQ and Social pointer

Compromise Issues & Internet Footprints

There exist multiple ways to access the internet, nonetheless it is recommendable that all detailed or sensitive internet research or open-source investigations should be undertaken on a covert or unattributed and registered PC, using a covert or unattributed internet connection. That is because the agency internet footprint could compromise an investigation or an intelligence operation. If both a covert and a not-covert user search for the same target, the covert user may then be linked to the not-covert user and therefore recognized as an investigator. Web pages can include images or adverts from third parties, which can leave cookies on your PC. Companies such as Ad-Image.com are able to compile a significant profile on you and your surfing habits, which are traded or sold to partners or customers.

Storage of Data and Gathering of Evidence

To ensure that a social media investigation produce high-quality, actionable intelligence, agencies must consider a number of issues, including which types of online content should be viewed and who will conduct the observation and analysis. Agencies might have to deal with a huge amount of data, and should count on social media extraction and visualization tools.

Many different laws may govern law enforcement agency records. Agency policy should cover the documentation, storage, and retention of social media information gathered for criminal investigations. Information gathered from social media sites should be printed and electronically archived. When saving and moving data the investigators must ensure that the evidential chain is preserved, in order to use the information as a proof.

In order to preserve the evidential chain, experts recommend making use of an MD5 or SHA1 Hash Extractor, software that retrieves the MD5 hash value (the digital thumbprint!) from file.

Privacy and Other Precautions

Law enforcement must avoid any appearance of collecting intelligence or information on individuals or organizations due to religious, political, or social views, or on any other grounds that could be regarded as violating the right against discrimination. Collecting data exclusively for those reasons can destroy confidence in law enforcement. Agencies must not use social media to collect information without understanding and following basic civil rights protections. Many agencies already have policies to protect civil rights and civil liberties. Agencies should include references to agency privacy protections when drafting social media policies to collect intelligence and conduct investigations.

Government Agencies' Databases (Publicly and Not-Publicly Available)

In many economies, local and state agencies maintain websites publicly available on-line, where the general public can retrieve information because policy, regulation, or the law permits the custodian of such information to do so. Users, and so investigators, are allowed to access hundreds of sources of current government information such as census data, judicial decisions, property and vehicle ownership records, property ownership, lien filings, company financial reports, salaries of public employees and a wide array of other information

for which an individual has little, if any, control over its public release.

Other public agencies and departments maintain registers not accessible to the general public, but may allow law enforcement agencies to access their databases, either directly, or through the appropriate administrative or judicial process. When instant access is not guaranteed, but Courts routinely grant access, a useful practice for the AOG may be to agree appropriate MoUs with different government departments to such end.

Financial information retrievable from public databases can be of high value for investigators. There are a great number of databases that could be used by a prosecutor or investigator in a corruption case. Given that a suspect frequents a certain residence, for example, public records could allow investigators to ascertain the ownership of the house, when it was bought, from whom and for how much, how the payment took place and who is paying taxes on it. As for corporations, public registers permit to gather information about when and where the company was formed, who are its directors or officers, and many other data.

Chapter 10. The Gathering of Private Digital Sources of Evidence and The Use of Digital Forensic Tools

Currently, large parts of human activities create some type of digital evidence. Digital evidence is not associated only with creating an email or writing a document on a computer. It can include surfing the internet or driving a car with a GPS, paying bills or using a video camera, withdrawing cash or using a copy machine: each of these actions creates digital evidence, and even activities that are perceived as not producing electronic evidence are eventually digitized at some point.

Significant digital sources of evidence in the investigation of corruption cases include:

- Computers
- Mobile devices
- Removable media and external data storage devices
- Online banking software
- Calendar(s)
- E-mail, notes, and letters
- Telephone records
- Financial or asset records
- Electronic money transfers
- Accounting or recordkeeping software

The importance of this enormous amount of evidence is that it can be recovered and used in criminal investigations, in asset tracing, and in any legal proceedings. Doing so requires a process of collection, preservation and analysis of electronic data that must then be presented for use in a litigation process.

Forensic acquisition and analysis of data techniques combine lost and tampered data with other digital evidence, allowing for easier identification, collection, preservation, analysis and presentation of evidence generated or stored in a computer. Additionally, as much of the day-to-day communication and financial transactions are conducted over the Internet, real time monitoring of bank accounts, e-mail traffic and the interception and processing of

other forms of on-line data become essential for conducting a proper investigation, complementing traditional investigative and surveillance techniques.

Since all these activities require the assistance of a digital forensic expert, the increasing trends have led to a huge demand for highly educated specialists in these disciplines.

Digital Forensics makes use of different methods and techniques, in order to deal with a variety of issues and to meet the diverse needs of investigations. It is possible, however, to summarize four essential elements or principles upon which every digital forensic technique relies on. It is therefore important when planning a case to have an expert in digital forensics who can effectively gather the digital evidence that is needed for the case.

Best Practices for Handling Digital Evidence

In dealing with digital evidence, the AOG must ensure that adequate procedures are in place, since every activity of investigation personnel exposes the evidence to the risk of accidental modification. That is why, in ensuring that evidence will be accepted in a court of law as being authentic and an accurate representation of the original evidence, the moments of collection and preservation of evidence are extremely critical. **(See Chain of Custody Chapter 8)**

Modification of evidence can have a devastating effect on the entire case, and therefore digital evidence needs to be protected and preserved all along the process collection, acquisition, analysis and presentation.

In the implementation of proper procedures and in the elaboration of training programs, agencies must apply the following general forensic principles:

- i. The process of collecting, securing, and transporting digital evidence should not change the evidence;
- ii. Digital evidence should be examined only by those trained specifically for that purpose;
- iii. Everything done during the seizure, transportation, and storage of digital evidence should be fully documented, preserved, and available for review.

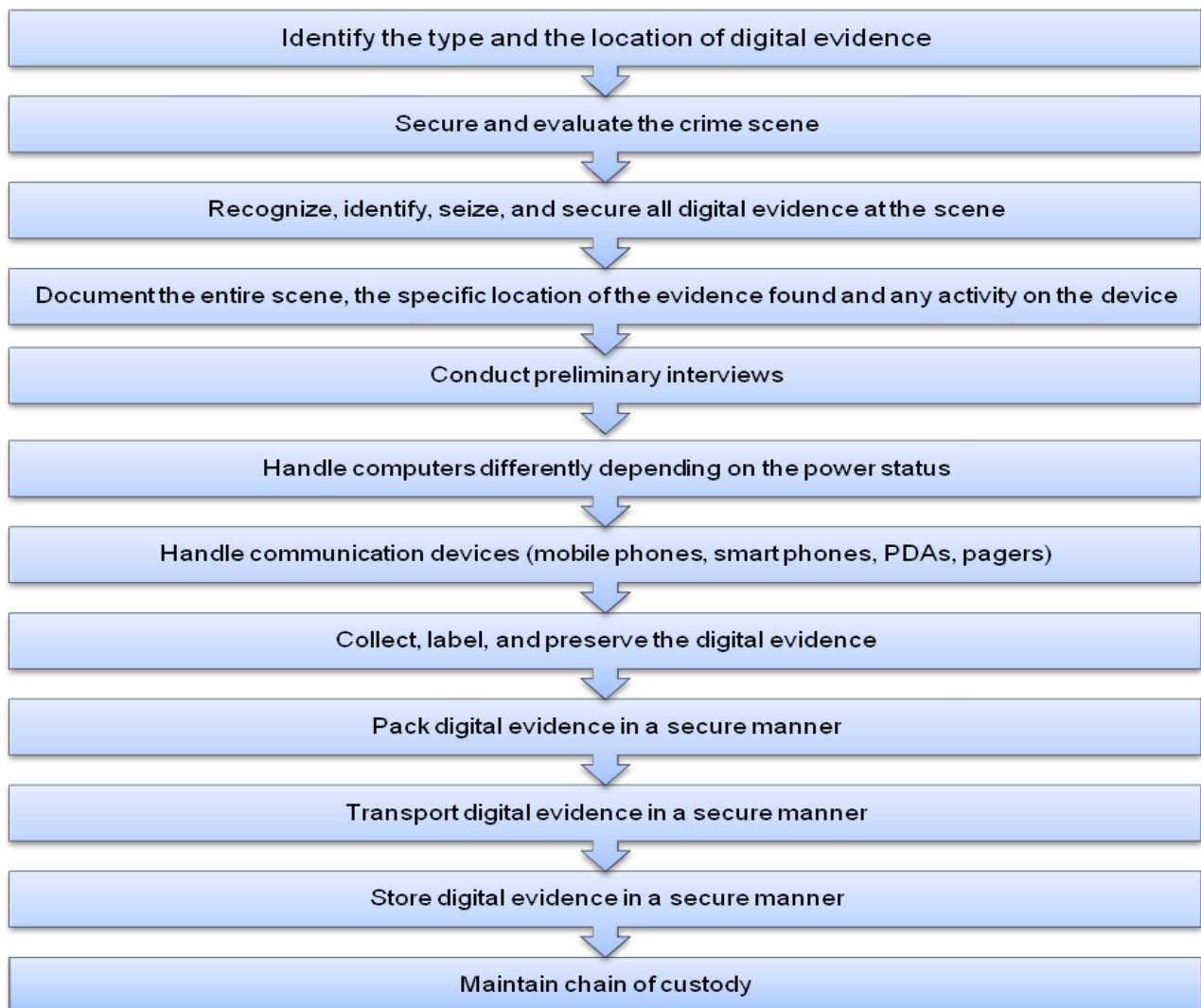
In the following sections, models are presented of those protocols and procedures that every agency should put in place for each critical stage in the digital evidence gathering

process.

Collection And Preservation of Digital Evidence

The collection step is critical since this is the first real contact with evidence. Not following proper collection procedures can lead to the destruction or modification of evidence, lost evidence, and subsequent challenges of the evidence collected. Some digital evidence requires special collection, packaging, and transportation techniques. Indeed, data can be damaged or altered by electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.

The following chart summarizes all activities that must be performed in the process of acquisition. Each activity will be detailed below.



Acquisition of Digital Evidence

Acquisition is the part of the forensic process during which actual data is copied or duplicated. Ensuring the integrity of evidence is the most critical part of the procedure.

Duplication

The only accepted method for duplicating electronic evidence requires that the original be protected from any possibility of alteration during the duplication process. This requires the use of accepted tools and techniques that allow the duplication of the evidence in a forensically sound manner.

Verification

This is the final step in the forensic copy process. In order for evidence to be admissible, it must be possible to verify that the evidence presented is exactly the same as the original collected.

E-mail

E-mail is one of the most abundant forms of evidence available for investigators. This is essentially due to a series of factors:

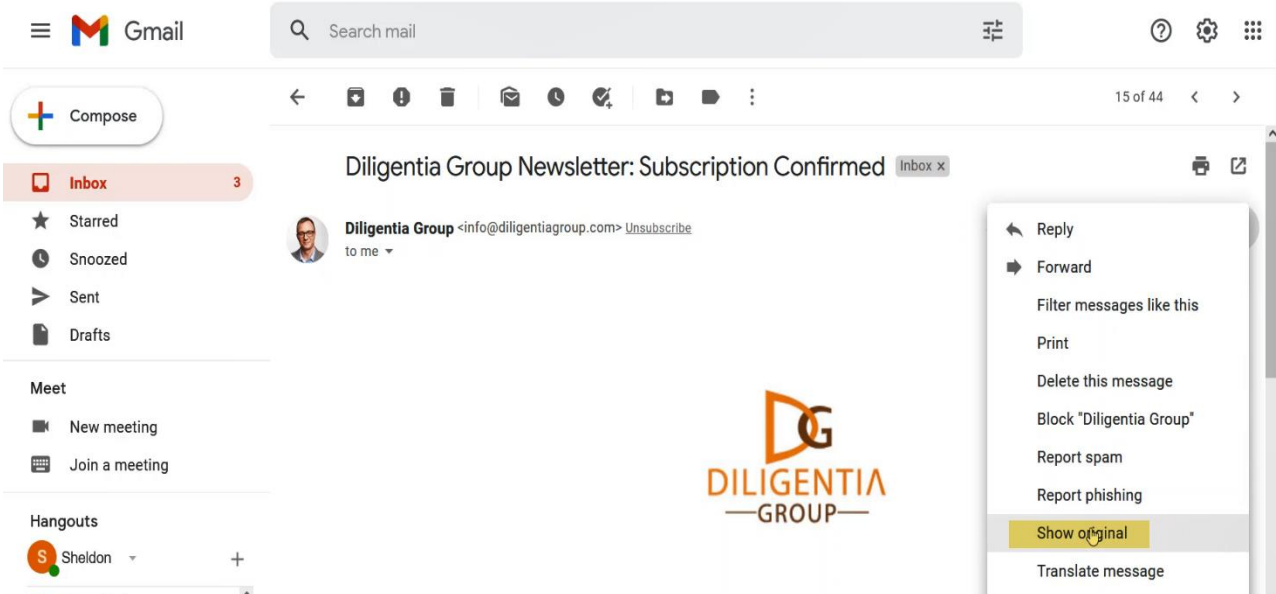
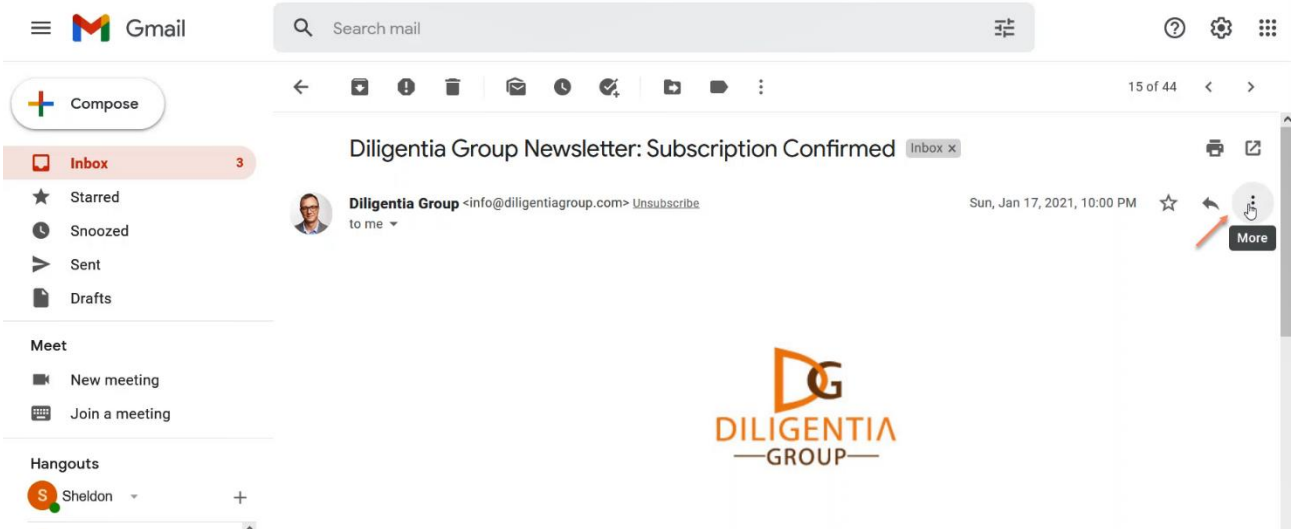
- i. Most people use e-mail informally and candidly;
- ii. Many people believe that e-mail messages are impermanent;
- iii. E-mails are more difficult to get rid of than most users believe, because of the ease of copying and forwarding, the fact that most e-mail systems require a two-step process to permanently delete e-mail from a system, and that the undeleted e-mails may be captured on system backups.

Emails can be stored in multiple and different places, depending on the type of account, providing multiple opportunities for investigators to recover email even when they have been somehow deleted.

The following summarizes all activities that must be performed in the process of email investigations:

1. Locate and Capture Headers or Message Meta Data

There are different methods to capture full email headers for various webmails (Gmails, Yahoo, Hotmail etc). For example, to capture the full email header in gmail, you click on the 3 vertical dots in the top right-hand corner and select "Show Original". See Image below.



Original Message

Message ID	<219dfd329047c9fd16157d8d1ba41d60042.20210118020027@mail9.mcsignup.com>
Created at:	Sun, Jan 17, 2021 at 10:00 PM (Delivered after 0 seconds)
From:	Diligentia Group <info@diligentiagroup.com> Using MailChimp Mailer - **CID3a6fab1550ba41d60042**
To:	slaawrence66@gmail.com
Subject:	Diligentia Group Newsletter: Subscription Confirmed
SPF:	PASS with IP 198.2.140.13 Learn more
DKIM:	'PASS' with domain diligentia.com Learn more

[Download Original](#)

```
Delivered-To: slaawrence66@gmail.com
Received: by 2002:a17:906:3655:0:0:0 with SMTP id r21csp355926ejb;
Sun, 17 Jan 2021 18:00:27 -0800 (PST)
X-Google-Smtp-Source: ABdhPJyBNFAMln/ppxPycsGAv705ovwKn3QrA5CbSAziqg65IUUVCGvz2NxluxrHNQk0JgdhnaIF
X-Received: by 2002:a25:7c06:1 with SMTP id x6mr33632806ybc.445.1610935227546;
Sun, 17 Jan 2021 18:00:27 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1610935227; cv=none;
d=google.com; s=arc-20160816;
b=wony76GppzWBq7E9V7Q9uOaxfz90zJYHfscfLOFLI1jg0IhnYps5GTy2IYwLwEX1
FMFMD4k28iLxjB9D8w6Ace5GY2YGHnFCK21AGke2m+W41IHP9UuY5u02xCSAH2bBEL
S2krWmmjLcRGiXoApq8Hn4fLnn+3gUjx17U/e3exz4aRS9uECQxuFP7EWDJovP448/Ey
C4wSjFU5FwULFbq31gqrTO+nT/Ry8ozYXw0jgYLArEXCelzBqWgQA/X14T6aAHUV5cBV
Nb/M9Ke25UJBNsYs2BT0StoyfIciannRit6yIzuJjDpp2vqsTcn26nrXUFTFOJf5pUd3
vtRw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=mime-version:form-sub:subject:message-id:date:to:reply-to:from
:dkim-signature:dkim-signature;
bh=hFYL/AbUShs5oDlpD2m9iEMvp0XlmgbxE4femvhWJJA=;
b=YFxm3m5RfVcnkxFI0P910zKaF7.13Vv-1.ct.3R+r1Hbhe1DnSv6KGTICOTU7FN5Pr+6I
```

Full email Header

2. Identify “Server” date and time of message as clients time/date stamps are less reliable.

Once the full email header has been captured, the Server date and time of message can be identified. See Image below

Original Message

Message ID	<219dfd329047c9fd16157d8d1ba41d60042.20210118020027@mail9.mcsignup.com>
Created at:	Sun, Jan 17, 2021 at 10:00 PM (Delivered after 0 seconds)
From:	Diligentia Group <info@diligentiagroup.com> Using MailChimp Mailer - **CID3a6fab1550ba41d60042**
To:	slaawrence66@gmail.com
Subject:	Diligentia Group Newsletter: Subscription Confirmed
SPF:	PASS with IP 198.2.140.13 Learn more
DKIM:	'PASS' with domain diligentia.com Learn more

3. Locate e-mail address of sender and recipient

Next, identify the email addresses of the sender and recipient. See image below.

Original Message

Message ID	<219fdf329047c9fd16157d8d1ba41d60042.20210118020027@mail9.mcsignup.com>
Created at:	Sun, Jan 17, 2021 at 10:00 PM (Delivered after 0 seconds)
From:	Diligentia Group <info@diligentiagroup.com> Using MailChimp Mailer - **CID3a6fab1550ba41d60042**
To:	slaawrence66@gmail.com
Subject:	Diligentia Group Newsletter: Subscription Confirmed
SPF:	PASS with IP 198.2.140.13 Learn more
DKIM:	'PASS' with domain diligentia group.com Learn more

4. Locate IP address of senders Node or the IP address of Mail server

The senders IP address is 198.2.140.13

Original Message

Message ID	<219fdf329047c9fd16157d8d1ba41d60042.20210118020027@mail9.mcsignup.com>
Created at:	Sun, Jan 17, 2021 at 10:00 PM (Delivered after 0 seconds)
From:	Diligentia Group <info@diligentiagroup.com> Using MailChimp Mailer - **CID3a6fab1550ba41d60042**
To:	slaawrence66@gmail.com
Subject:	Diligentia Group Newsletter: Subscription Confirmed
SPF:	PASS with IP 198.2.140.13 Learn more
DKIM:	'PASS' with domain diligentia group.com Learn more

5. Locate the Message ID.

The message ID is used to uniquely identify the email and determine its authenticity. Please see image below.

Original Message

Message ID	<219fdf329047c9fd16157d8d1ba41d60042.20210118020027@ma
Created at:	Sun, Jan 17, 2021 at 10:00 PM (Delivered after 0 seconds)
From:	Diligentia Group <info@diligentiagroup.com> Using MailChimp Ma
To:	slaawrence66@gmail.com
Subject:	Diligentia Group Newsletter: Subscription Confirmed
SPF:	PASS with IP 198.2.140.13 Learn more
DKIM:	'PASS' with domain diligentia.com Learn more

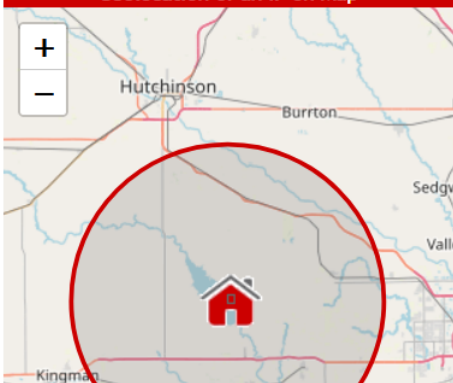
6. Perform a reverse lookup on sender's IP address

Using a reverse lookup tool, we conducted a search of the sender's IP address and narrowed in on the location of the sender's server.

Enter an IP or domain name and start tracing and finding the IP location with our free tracking tool.

198.2.140.13

Trace IP With IP Tracker

Geolocation of an IP on Map	Basic Tracking Info
	<p>IP Address: 198.2.140.13</p> <p>Hostname: mail9.mcsignup.com</p> <p>Internet Protocol: IPv4 - Version 4</p> <p>Types: Public</p> <p>IP Classes: Class C Range (192.0.0.0 to 223.255.255.255)</p> <p>Reverse DNS: 13.140.2.198.in-addr.arpa</p> <p>Blacklist Check: Blacklisted. Active in Spam 17 days a go [198.2.140.13 Blacklist Check]</p>

7. If only a mail server is identified, evoke the relevant legislative framework to obtain user identification data using Message ID

With the information you obtain (full email header including the message ID), evoke the relevant legislative framework to obtain user identification data. Ultimately, subpoenaing Gmail to produce the data you require.

Securing the Evidence

The Examiner must print a master copy and two working copies of the original email and its full email header. The master copy must be exhibited and stored in the evidence room for presentation in court/tribunal.

Admissibility of Email Evidence

The proponent must show the origin and integrity of emails - the hard copy of the e-mail evidence is consistent with the one in the computer and includes all the information held in the electronic document.

Chapter 11: Human Intelligence

People are a rich source of information in any investigation since the very object of investigations is always the human behavior. This is the reason why intelligence derived from information collected and provided by human sources is essential in every kind of investigation, and why, even in the digital era, human intelligence sources remain one of the key operational tools for law enforcement and investigative agencies.

Suspect Profiling

When planning an investigation into a possible fraudulent conduct committed by an individual or a corporation, it is essential to identify the key information – and the related key questions that are needed to set the ground for a deeper comprehension of the alleged facts and the suspect 's profile, as well as to further develop the case.

Identifying key questions and target information is critical in order to establish a priority order among the sources of information to be consulted and the investigative actions to be taken. This also allows channeling the limited resources only to those selected leads which may result in the development of the most significant evidence in a timely manner.

Basic information can be organized into six categories, corresponding to six key questions about the alleged facts under investigation. These are the Who, What, Where, When, Why and How already detailed above.

When dealing with suspects of corruption, investigators should focus on those elements that have proven to be common in the stipulation and execution of a corrupt agreement.

The Briber: Private Individual or Entity

- All official data on the company: Trade Register; Stock Exchange
- Organizational charts for an adequate period of time, in particular:
- Location of the sales/marketing department
- Job descriptions, liabilities and executive powers in the company during the relevant time and in the relevant area
- Data on money flows through bank account inquiries
- Information on sales agreements

<ul style="list-style-type: none"> • Compare those data with similar companies' data (business analysis) • Expenses recorded in the nominal ledger • Performances of sales and marketing staff:
<ul style="list-style-type: none"> • To whom they have sent invitations? • What kind of hotel bills, parking tickets, lunch receipts, flight tickets or bus tickets have been entered in the accounts? (this information can provide important insights about people involved) • Cross checking the receipts with agents' and other suspects' receipts might provide good evidence • Use of third-party agents • Has the agency- relationship been registered? • Where is the agent established? • Where, how and how much has he been paid? • How have those payments been recorded?
<p>The Bribed: Public official</p> <ul style="list-style-type: none"> • Public official income • Wealth disclosure statement • Job, income, wealth and other financial information about his family members • Place of residence • Activity of his office • Family house ownership and acquisitions • Cash flow analysis • University tuition of familiars • Vehicle ownership • Travels • Real estate ownership • Employment of family members • Academic tuition for family members

The investigators should be able to prioritize leads and information which may allow development of strong evidence against the offenders, for example:

Personal Residence

The personal residence ownership and acquisition transaction can reveal important information about the financial situation of the public official. A significant difference among the value of the purchase and the actual bank loan can reveal a very large initial payment at the time of purchase. Financial information relating to the purchase may be obtained where the property had been purchased through a licensed conveyancer and the loan

obtained at a major bank. For example, the bank may maintain detailed records of the transaction, having financed a significant amount and conducted due diligence which may reveal the source of the initial payment. The conveyancer may also have records of the complete transaction. The seller of the property should also be interviewed to obtain the complete details of the transaction, including the method of payment for the house.

Cash Flow Analysis

If the public official maintains a bank account at a domestic financial institution, the records of this account should be requested very early in the investigation because it may require a significant amount of time for the bank to research the records. If the government salary of the public official has been deposited into this domestic account, it will be important to perform a complete analysis to establish how his legitimate salary has been spent. A cash flow analysis relating to any cash withdrawals or deposits should also be prepared. Once these financial flows have been analyzed, it will create a complete picture of the distribution of his legal funds and show how much cash was available for purchases. This may be very significant if expenditures are later identified from unknown or illegal funds. Large cash payments or purchases from unknown sources may be an important piece of evidence at trial.

University Education

A common way to reward a corrupted official has proven to be the coverage of college and university tuition for children and other relatives of the public official. Investigations into the public official's family members may reveal, for example, that his sons are attending prestigious university abroad and there is a very good chance that the official is not able to afford the corresponding tuition, living expenses and travel costs. In this case, investigators should try to determine whether a legitimate source of funding, such as a scholarship granted by the university exists, and who is actually paying the university tuitions. The universities should therefore be contacted, the expenditures documented and the source of payments identified.

Vehicle Ownership

Another major lead from the pre-investigation activities might be vehicle ownership of the public official or of his family members. For example, the fact that the public official's wife

owns an expensive automobile is an indication that he may be living above his means. Investigation into the purchase of the vehicle purchase will involve first tracing the ownership of the car to determine the prior owner. This can lead to the records of the transaction, who was the purchaser, the date of the purchase, and – the most important – the source of the payment. If the payment were made by bank check, the dealership may have a copy of it. Payment made by cash is noteworthy evidence if, for example, the cash analysis of the public official's bank account has established that he did not have available a corresponding amount of cash from his legitimate sources of income.

Informants and Suspects

For investigations into corruption cases, human intelligence resources are particularly invaluable in circumstances where there is a real lack of information about the corrupt network. In cases of serious economic offences and corruption, the individual who comes forward may well be a disgruntled former employee, a whistle-blower, a company representative who has been cheated out of a procurement deal by large- scale bribery or even a former co-conspirator with an axe to grind.

Investigators must nevertheless pay careful attention to the reliability of these sources of information by considering the reasons and the motives for the individual wishing to pass on information. The investigator must consider whether those motives might be malicious and therefore misleading, and whether an inducement was sought for providing the information. These all have the potential to compromise the investigation. Accordingly, investigators should seek to corroborate the information provided by informants through other sources of evidence and investigative tools.

When dealing with informants and witnesses, a comprehensive strategy should be developed. The following areas should be addressed:

Informants And Witnesses

Provisions should be in place for the protection of witnesses. Witnesses' identities should remain confidential for as long as possible. Witness relocation or protection programs or a new identity program may be available. If the witness is in prison, provisions for a safe location must be established. The appropriate policies need to be developed as soon as

possible so as to be in place when the need arises.

It is advisable to reduce opportunities for the defense lawyer to attack the credibility of the witnesses (by having recorded statements, transcribed and signed or initialed by the witness). Processes should be established to deal with lawyers who are either attached to the witnesses or to the potential defendants. If the witness has a criminal background, it is important that they are open about prior criminal activity (particularly if it involves the defendants) and to ensure sure that this information is disclosed to the court prior to the witness undergoing examination. Keeping witnesses informed of the criminal prosecution process will instill confidence in them and allay fear and apprehension.

Specific considerations are to be made with reference to the different categories of informant and to specific needs.

Confidential informants

They are generally criminals. Unlike a cooperating witness, their personal information must be maintained as confidential. The motives of the informant may be revenge, financial gain, or personal protection (i.e., to avoid being sentenced to prison). It is important to note that confidential informants are almost never expected to testify in court.

Confidential Sources

They are generally not criminals, but they provide information because of their position or employment. Attention must be given to safeguarding these sources' income to prevent it from being jeopardized due to interaction with investigators.

Cooperating Witnesses

Cooperating witnesses supply their information in a confidential manner, but they are expected to become witnesses. Remember the importance of protecting witnesses. When using a source or witness, as described above, internal protocols and procedures need to be established as uniform policy. The following elements are important: -

- Written agreements used to define the responsibilities of both the source and the law enforcement agency
- A system of either code words or names established that will be used in files to prevent accidental disclosure

- Original information kept separately from the general investigation files
- Limited access to the source files for those within the investigative agency
- Routinely audited financial records associated with source operations
- A third-party present when payments are made to a source and receipts obtained
- Periodic reviews, at a managerial level, of the source files as an internal audit protection
- Any promises being made to the informant or witness cleared with the government agency or government attorney (It is good policy to have all promises in writing to protect the integrity of the investigator and the investigative process)

Protection of the Source/Witness

Threats to the source or witness should be anticipated before they actually occur, and the investigative team should be prepared to immediately respond. A threat assessment should always be performed for witnesses, and it must always be determined if the witness is fearful of an approach or an act against their person. There are two approaches to threats to witnesses:

- A reactive approach is the aggressive investigation of any threat or act of violence to a source. During this approach, no intimidation of any witness is tolerated
- A proactive approach involves having witness assistance and witness protection programs available. It is important to remember that most witnesses are frightened simply by being involved in a criminal process. These concerns need to be dealt with by the team

Chapter 12. The Gathering and Analysis of Financial and Corporate Evidence

The success of any corruption or money laundering investigation depends largely upon the ability of the investigator to track the ownership trail of money and other assets that leads away from the crime or the criminal activity. In other words, the first step in the process of asset recovery is to trace the proceeds of crime or assets subject to confiscation. Integrated financial investigation is an essential element of any strategy targeting the proceeds of crime. A recognized best practice is to integrate the criminal investigation team with forensic accountants and financial investigators.

Tracing and Identifying Financial Assets

The investigation of large-scale corruption cases should follow the money trail in order to establish links between the stolen assets and the proceeds-generating criminal conduct. In complex financial crimes, the asset to be linked to the offence is more likely to be the product of an intervening transaction. As a result of the intervening transaction, the asset is in a fungible form, which makes it easy to exchange for a different asset. Tracing the proceeds of crime is premised on the assumption that the criminal origin of assets can be concealed through transformation, and that transformed assets can easily and speedily be moved between locations or across borders. The assets can be mingled with others and converted into other forms.

When the assets are the proceeds of an offense, they will often be moved around the world using different schemes, such as off-shore centers, corporate vehicles and a variety of financial transactions in an effort to launder the funds. Hence, investigators should be able to obtain information from financial institutions regarding financial transactions, pierce the corporate veil of a corporate vehicle to determine the ultimate beneficial owners and be capable of analyzing the obtained information.

Access to Financial Information

One of the most persuasive evidence in a corruption case is evidence that a person benefited financially from his allegedly corrupt activity. For example, evidence that the

person deposited large sums of cash into a bank account, purchased expensive items with cash, or spent significantly more money than can be attributed to legitimate sources of income. **(For details on gathering financial information see Chapter 9)**

Gathering Information of Corporate Vehicles

The proceeds of an offense are usually hidden using a corporate vehicle (companies, trusts, foundations, fictitious entities or unincorporated economic organizations) to disguise the criminal's role as the beneficial owner i.e., the natural person who ultimately owns or controls the assets or the bank accounts of the corporate vehicle. However, many governments are demanding greater transparency about beneficial ownership and accordingly, have begun to require the public disclosure of beneficial ownership information, that is, to reveal the identity of individuals who ultimately enjoy the benefits of property rights, even if they are not legal owners. The lack of transparency allows various illegal activities such as e.g., tax evasion and corruption

Where there is no transparency of beneficial ownership, the investigator will need to prove the link between the corporate vehicle and the beneficial owner. If the company is registered, the company registries are the entities that collect and store information on the structure and individuals that own and manage the entity. This information includes: the name of the company, legal entity type, the address of a registered office, the physical location or principal place of business, the names and addresses of a registered agent, person authorized to accept service of process, or a resident secretary, the names and addresses of persons in positions of legal control within the legal entity (directors and officers), and the names and addresses of persons in positions of legal ownership (shareholders or members). One flaw of the information held by companies' registries is that sometimes it is not completely accurate or it is not kept up to date (quality assurance and updating are usually responsibilities of the legal entities).

In recent years, many registries have begun to upgrade their systems to take advantage of recent developments in digitalization and electronic processing. Furthermore, information regarding the name of the corporate vehicle, the documents incorporating the company, the names of the board members, and the names of the persons entitled to conduct business on behalf of the company are often held by service providers. These

institutions are internationally obliged to conduct customer due diligence of the corporate vehicles to which they provide services.

Since the investigator will have to determine who ultimately effectively controls a corporate vehicle, it is useful to consider the type of corporate vehicle that is being analyzed:

Corporate Vehicle	Persons Having Ultimate Control
Companies	The shareholders, the board of directors, the executive officers.
Trusts	The trustee, the settlor, the beneficiary.
Foundations	The director or board, the private beneficiary

A typical obstacle to obtaining information about corporate vehicles is that -the relevant documentation may be deliberately dispersed across different jurisdictions. Collecting information on a particular legal entity that is incorporated or formed under the laws of Country A but administered from Country B often entails first submitting a request to Country A and then submitting a request to Country B.

Furthermore, if the company is an international business corporation (IBC), a structure typically used for shell companies (set up by non-residents in off shore financial centers OFCs), obtaining information about them tends to be much more difficult since they usually have no economic activity and, if used illicitly, additional mechanisms are used to obscure the beneficial ownership, such as exercising control surreptitiously through contracts, adding layers of corporate vehicles to obscure the beneficial ownership, hiding behind bearer shares and ensuring that the beneficial owners are located in another jurisdiction.

The challenge when investigating IBCs is to pierce the corporate veil and find the beneficial owner (the person who controls the company and its assets). To do this, investigators can ask information about the real owner to the jurisdiction where the company is registered. However, in offshore centers, the registry, where it exists does not often require the actual identity of the beneficial owner.

Consequently, in gathering information of corporate vehicles, investigators have access to publicly available information, law enforcement databases, information held by entities such as financial intermediaries (banks and other financial institutions) and, companies 'registries, among others. Investigators also engage useful tools such as their compulsory powers (disclosure, search, and seizure) and mutual legal assistance.

However, investigators usually encounter obstacles identifying the beneficial owners of involved corporate vehicles due to different factors. First, the lack of availability of beneficial ownership information in a given jurisdiction because, for example, it is not required by the corporate registry or a corporate service provider, or because of stringent bank secrecy or other anonymity laws that impedes access to beneficial ownership information held by some institutions. Secondly, the type of corporate vehicles such as IBCs (which are not required to have a physical presence in the jurisdiction of their formation) or Limited Liability Corporations (whose simple structures allow for formation with as few as one member). Additionally, bearer shares, layering and multiple jurisdictions, as well as the lack of harmonization of international standards regarding covered entities under domestic AML regimes are other challenging obstacles to be overcome.

Analyzing Financial Evidence

After tracing and identifying the assets, the analysis of the evidence is the next step to prove the illegal trail of the assets.

There are different types of methods for proving the receipt of unlawful income that an investigator could use in a corruption case. The type of evidence available will dictate which method is most appropriate for a particular case. These methods could be direct, such as the specific item method, or indirect, such as the net worth method or the source and application of funds method. Some of these methods are;

Specific Items Method

The specific item method is used when there is evidence that can directly trace the flow of money from the corrupt activity to the official. For example, when the investigator has a witness who can testify that he carried bribes to a public official on behalf of a third party or paid the bribes directly to the official on behalf of himself, this evidence constitute

specific item proof that will support a corruption charge. Or when a bribe was paid sending a wire transfer from the company's bank account directly to the bank account of the public official. This type of evidence is often used together with an indirect method of proof (whether a net worth method or the Source and Application of Funds method) which uses circumstantial evidence to support a corruption charge.

Net Worth Method

The net worth method is an organized process by a Law Enforcement Agency in which intelligence is gathered to determine if public officials are living significantly above their legitimate means. The project is not an initiation of criminal proceedings; it is merely the collection of public and government database material and other non-public law enforcement information relating to a group of public officials, such as all persons at or above Deputy Minister level or all procurement officers. This data is used to make a comparison of total assets owned by a person relative to their tax returns and asset declaration statements. If the computation discloses a significant increase in the net value (excluding appreciation) of assets that is many times more the known and legal income of the official, then the possibility of corruption may have been detected. Additional information will be needed to further support this suspicion.

The net worth method is often used in situations where an individual invests illicit gains in property such as stocks, real estate and business ventures. The investigator will have to prove that the suspect has underreported income (i.e., there are discrepancies between an individual's income for a given period and their net worth). First, it will have to establish the person's opening net worth or total net assets at the beginning of the period that is being investigated. Next, the investigator will have to present evidence of the increase in the suspect's net worth over the investigated period. The source of this increase has to be a taxable one, such as the receipt of bribes. The evidence could also include the lack of non-taxable sources of funds in the investigated period that could account for the increase in net worth (gifts, inheritances, loans, etc.). Finally, the unreported income that represents the bribe or the unlawfully-derived income will be the difference between the reported income of the suspect and the increase in net worth for that period.

The Source and Application of Funds Method

The Source and Application of Funds method of proving the amount of illegal income is used when direct evidence is not available, and the investigation discloses that the subject spent far more money during a set period than he had legally available to him. This set period of time can be any amount of time that demonstrates an increase in spending or wealth far above the legal means of the subject. The basic theory for this method is that the person under investigation spent far more money during a set period of time than he had legally available to him.

The total and cash expenditure methods are the most useful methods of financial proof in a corruption case. These methods are usually employed in typical corruption cases where the person spends the unlawfully obtained cash on consumable items (food, entertainment, clothing, travel, or other items that are not traceable, such as cashier's checks, money orders, traveler's check, etc.).

In the total expenditure method, the prosecutor or investigator should calculate a starting point, reflecting how much cash the suspect had at the beginning of the investigated period, through financial statements, loan applications, financing arrangements, economic disclosures statements, admissions made to investigators, or a review of their financial condition prior to the charging period. And then, the person's expenditures for the given period should be totaled – the investigator or prosecutor should look for increases in cash deposited into the suspect's bank accounts, cash purchases, checks written, third-party checks issued to the suspect, personal expenditures etc. If those expenditures exceed his reported income for the investigated period of time and the available cash at the beginning of that period, the excess represents the amount of unreported unlawfully-obtained income that constitutes the basis of the investigated criminal conduct.

The cash expenditures method deals solely with the suspect's use of cash, which include withdrawing cash from a bank account, receiving cash loans, writing checks for cash, cashing salary or third-party checks, etc. By calculating all of the person's cash expenditures and subtracting all legitimate cash sources, the prosecutor can conclude the amount of cash expenditures that exceeds the legitimate sources of cash for the investigated period, which represents the cash bribes, payoffs, or otherwise illegally

obtained funds resulting from the suspect's corrupt conduct.

It is often used to create a prima facie case that the individual is corrupt. The investigator or prosecutor has to establish the disproportionate income, property, or assets. When material possessions are of an amount or value so disproportionate to the person's official or other earnings, the burden of proof shifts to the suspect who will have to prove the lawfulness of the sources from which he has acquired those possessions. It must be proved that the suspect maintained a standard of living not commensurate with present or past reported salary, or with benefits, during the investigated period. Special attention should be paid to the fact that the suspect's relatives or friends might be the ones in charge of the control of the property or assets on the suspect's behalf.

In summary, it is necessary to prove the disproportion among the property, the amount of monetary resources or assets that were controlled by the suspect during the investigated period, and the total payments made during the same period. Additionally, all outgoing payments and capital additions, both domestic and abroad, should be analyzed, which includes:

- Goods and services acquired during the investigated period;
- Running costs, expenses of repairs, or maintenance and outgoings, incurred during that period (and/or connected with the property acquired before that date);
- The value of any gifts given;
- The money spent by the suspect on another individual;
- The ability to obtain credit during the given period
- The value of services obtained on credit
- Prepayments that were made during that period;
- Total amount of salaries or hires paid during the period;
- Bills remaining unpaid for goods and services rendered during the period;
- Increase in the defendant's bank account between the beginning and end of the period being investigated;
- Deposits and investment made by or for the defendant, family, etc.;
- Payments made by third parties for the benefit of the defendant;

- Credit given for money received from sale of assets or goods before the charged period (if shown they come from an untainted source); and
- All sources of income.

Furthermore, the suspects might also have accounts at banks separate from those where legitimate sources of income are deposited; hence, the prosecutor or investigator should require the suspect 's bank information from all the financial institutions in the areas where the person lives, works or has any connection, such as a vacation home.

Analyzing Bank Records

The analysis of bank records is an essential task in a financial investigation. Although it could be seen as a complex and difficult task, even nonfinancial experts are able to conduct some initial analysis. These initial steps are:

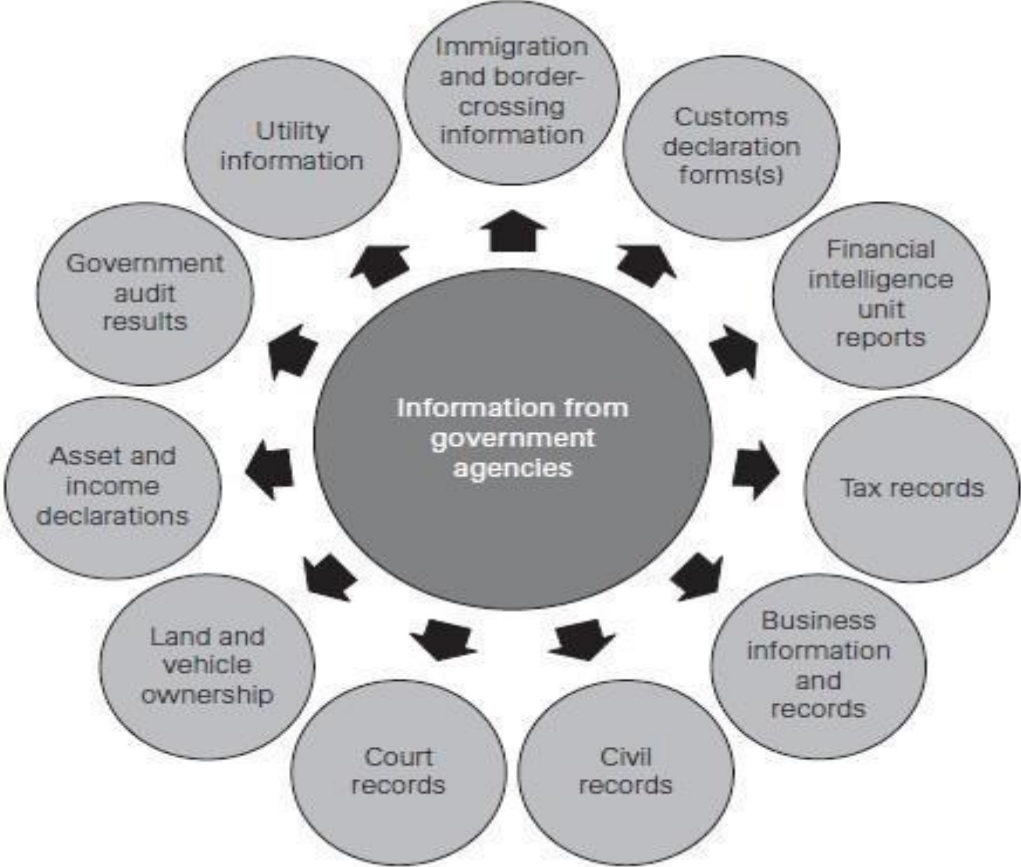
- First organize the records in an electronic database (i.e., an Excel spreadsheet). Once all data from the bank account has been entered into the spreadsheet, either manually or by a computer process, the analysis will be divided into three relatively easy tasks, namely the analysis of the deposits, the analysis of the disbursements and the identification of balances on certain dates.
- The deposit analysis will include reviewing each item deposited into the account and determining its source: legal, illegal or unknown. For some deposits, such as salary payments, their type (legal, illegal or unknown) may be easily determined by simply reviewing the bank documents. However, if the source is unknown, the investigator will have to make third party contacts to inquire about the purpose of the payment that was made to the subject. By developing a list that summarizes and totals each type of deposit, the investigator can focus on what leads are most important to follow.
- The analysis of the disbursements can be accomplished in the same manner. The investigator can now quickly identify which items require additional follow-up or detective work. This disbursement analysis assists in identifying assets purchased, business associates, transfers to other bank accounts, international money movements and spending that exceeds the subject's legal income.
- In some cases, it may be important to identify the balance that is in the bank account

on a particular date or on a series of dates. This also can be quickly accomplished by adding a column in the Excel spreadsheet that automatically calculates the balance following every transaction.

- These are the three basic types of analysis that should be completed for each bank account. In addition, there are other records maintained by banks that should be reviewed, such as account opening documents, bank due diligence reports, loan files, electronic funds transfers and correspondence files.

Obtaining Overseas Assistance

In the process of asset tracing, it is often the case that crucial information is located in another jurisdiction. Therefore, obtaining assistance from a foreign country is crucial for the success of the financial investigation. The figure included below shows the preliminary information available from other foreign agencies:



Information from government agencies

SOURCE: Source: StAR Initiative, Asset Recovery Handbook. A Guide for Practitioners, 2011, p. 49, Figure 3.2, available at: <https://StAR.worldbank.org/StAR/sites/StAR/files/Asset%20Recovery%20Handbook.pdf>.

Most APEC Economies have ratified the United Nations Convention Against Corruption, which serves as a basis for legal mutual assistance in the investigation of corruption offences. In addition, several MLA treaties and domestic legislation of the APEC Member economies expressly require the economy to trace and identify proceeds of crime in their jurisdiction upon request from another member. Often, the tracing and identification of assets do not involve any special MLA procedures but only the gathering of documents. However, some APEC economies have additional measures designed specifically for the tracing of proceeds of crime.

Some jurisdictions disclosure obligations are a barrier to MLA requests since it obliges authorities to provide notice to the targets of those MLA request, granting the targets the right to appeal a decision to provide the assistance. This requirement implies a risk for the financial investigation; it could lead to the dissipation of funds and to lengthy delay (the target will try to block the process and use all legal barriers at his/her disposal to exhaust all instances of appeal).

Some proposals to circumvent this barrier are:

- Discuss issues and strategy with foreign counterparts;
- Consider conducting a joint investigation or providing information to the foreign authorities so that they can conduct their own investigation and take provisional measures. Either option may remove this potential avenue for delay because disclosure to a target can be postponed for domestic investigation and provisional measures;
- Ensure that a request is not overly broad to prevent potential arguments that the request breaches privacy;
- Ensure that facts and reasons for the request are outlined clearly to address potential arguments that the dual criminality test is not met that is, a target may argue that the request is a tax investigation colored as a corruption investigation and intended to go around the dual criminality principle.

Chapter 13: The Basic Steps of a Complex Fraud and Corruption Investigation

Investigating fraud and corruption can be a very tedious task, this is so because of the layers that are involved in this activity. An investigation can commence from a private capacity, however when agencies lack law enforcement powers to compel evidence from third parties by subpoena or otherwise, they can, expand their access to evidence by referring cases to law enforcement agencies for assistance. AOG investigators should be aware that the fraud theory approach discussed in Chapter 1 will be applicable when carrying out these investigations.

Learn The Elements of Proof for The Suspected Offenses

Memorize the elements of proof for each of the suspected offenses, based on your theory of the case, and use them to organize the investigation and test the sufficiency of the evidence. An investigator should know at every stage of the case what evidence he needs to obtain to prove an offense. Again, many investigators neglect this fundamental rule, with the result that too little (or too much irrelevant) evidence is collected.

Carefully Organize and Maintain the Evidence

Use charts and graphs, spreadsheets and summaries as necessary to organize and analyze complex data, but be careful not to overdo this exercise at the expense of having time to pursue leads and pursue your theory of the case. Make sure that all evidence is properly logged in, secured and accounted for, including electronic evidence, and that the source of the evidence is recorded; ensure a proper chain of custody is maintained.

Prepare The Case Chronology

Preparing a chronology of events putting the important facts in the order they occurred is always helpful, particularly to prove knowledge and intent and to see how a case unfolds. Concisely record the date, the event or Document, and the source of information in separate columns. Include important meetings, telephone calls, email communications, travel, key documents and other potentially important events. Keep the chronology simple and focused on potentially relevant evidence as too much extraneous information will reduce its utility; review and update it regularly. Add new information as the investigation proceeds and remove what is shown to be irrelevant.

The Basic Steps of a Complex Investigation

The information below illustrates basic steps in a typical complex procurement fraud case. Most significant fraud and corruption cases occur in procurement.

The steps below assume that your case begins with a complaint about the procurement process, without any specific information about possible illegal payments or fraud. If so, your investigation would typically begin by examining the procurement process to identify leads and eventually evidence of bribery, collusion or other wrongdoing. This is the way most such cases begin and are organized.

In other cases, your investigation may begin with reports that a public official is displaying unexplained wealth or living beyond means, suggesting possible corruption, without reference to any particular procurement abuses. In that case you must reverse the investigation process by first identifying the illicit financial transactions and then tracing them back to the underlying procurement transactions, if necessary. See Step Seven below for more information on this approach.

Step One: Begin the Case (Respond to Complaint, Etc.)

If the case starts with a complaint or report, fully debrief the complainant, getting as much detail as possible. If the case starts with the discovery of a red flag, match the red flag to the potential scheme and then look for other red flags of the suspected schemes. An automated, “proactive” search for fraud indicators might be effective if the necessary data is available.

Step Two: Evaluate the Allegations or Suspicions

Determine whether the allegations or suspicions – the “red flags” – are specific and serious enough to justify an investigation, which can be time consuming, disruptive and costly. If you determine that a complaint or report warrants further investigation, try to make a quick, preliminary assessment of the accuracy of the complaint. For example, if the complainant alleges that he or she was unfairly disqualified from a tender, examine the relevant project files to attempt to determine if this may have occurred. Use this information to prepare for the follow up interview of the complainant.

Step Three: Conduct due diligence background checks

Check on-line and other records on the suspect firms and individuals to evaluate the allegations and to look for other evidence of fraud or corruption, such as the presence of

shell companies as subcontractors, prior debarments of a contractor or evidence that a project official is living beyond his means.

Step Four: Complete the Internal Stage of The Investigation

Complete the collection of documents, data and interviews within the investigating organization, e.g.,

- Look in the bidding documents for evidence of corrupt influence through the manipulation of the “SPQQD” factors – Selection, Pricing, Quantity, Quality and Delivery;
- Carefully examine bids and proposals, CVs and other documents submitted by a suspect firm for possible fraudulent representations;
- Access, with the proper authority, the relevant e-mail and computer hard drive information;
- Determine if an early interview of the subject is warranted.

Step Five: Check for Predication and Get Organized

Review the results of the investigation to date to determine if there is adequate “predication” a sufficient factual basis to proceed. Decide or refine your initial “Fraud/Case Theory” and organize the evidence according to the elements of proof of the potential claims. If law enforcement assistance is needed (e.g., to subpoena documents, exercise search warrants or to request international legal assistance) take steps to ensure that there is sufficient “probable cause” to obtain such cooperation.

Step Six: Begin the External Investigation

Conduct interviews of witnesses outside the investigating organization, proceeding from the disinterested, cooperative witnesses to “facilitators” to co-conspirators to the subjects. Request or compel documents from third parties and the suspect contractors through negotiated agreements, the exercise of contract audit rights or, if available with law enforcement assistance, subpoenas or search warrants.

Step Seven: Prove Illicit Payments

Determine the best strategy to prove illicit payments: out from the point of payment (by examining the contractor’s records), or back from the point of receipt (from the suspect employee’s records) and begin the tracing process. If it is not possible to prove the corrupt

payments directly, try to prove them circumstantially by showing the subject displayed unexplained sudden wealth or expenditures.

Step Eight: Obtain the Cooperation of An Inside Witness

This could be an honest inside observer or a lesser participant in the offense, such as a middleman or the smaller of several bribe payers. Decide the best strategy to obtain his or her cooperation.

Step Nine: Interview the Primary Subject

In a corruption case, conduct a thorough interview of the primary subject, usually the suspected bribe recipient. Ask about his role in the suspect contract award and relevant financial issues, such as his sources of income and expenditures. Decide if there is sufficient evidence to obtain a confession, which is unlikely; otherwise, try to get helpful admissions, information on the subject's source of funds and possible defenses. Record the interview, if possible, and request all relevant financial and other records.

In a fraud case, interview the person most knowledgeable and responsible for the suspected false statement or fraudulent document. Again, decide if there is sufficient evidence to obtain a confession and, if not, try to get helpful admissions and identify possible defenses. These typically include that any false statement was an honest mistake, or that another person was responsible for a fraudulent document.

Step Ten: Prepare the Final Report

Decide what action to recommend based on the results of the investigation – an administrative sanction or criminal referral, for example – and prepare a concise final report, organized according to the elements of proof for the relevant offenses.

Chapter 14: Conducting Effective Interviews

Interviews are a key component of any investigation. It is from this medium that evidence is gathered and verified. That information may be used or provided to other authorities immediately or later.

Interviews can be unstructured, free-wheeling, and open-ended conversations without predetermined plan or prearranged questions. One form of unstructured interview is a focused interview in which the interviewer consciously and consistently guides the conversation so that the interviewee's responses do not stray from the main research topic or idea.

Interviews can also be highly structured conversations in which specific questions occur in a specified order. They can follow diverse formats; for example, in a ladder interview, a respondent's answers typically guide subsequent interviews, with the object being to explore a respondent's subconscious motives. Typically the interviewer has some way of recording the information that is gleaned from the interviewee, often by keeping notes with a pencil and paper, or with a video or audio recorder. Interviews usually have a limited duration, with a beginning and an ending.

Gather Information

An investigation interview is designed to gather information about an incident and find the truth, not necessarily to elicit a confession or eliminate someone as a suspect. Developing effective interviewing skills involves training and practice and studying the elements of human communication is a great way to work on these skills. Some of the most important concepts in investigation interview training include detecting deception, eliminating bias, and building rapport with interview subjects.

A good investigation interview is only as good as the person conducting it. As with all skills, practice makes perfect, but there's no harm getting a bit of help along the way. Follow following tips to get the most out of your interview subjects.

Preparation

- i. Pick a non-threatening place for the interview, such as a conference room or private office.

- ii. Give the interviewee a choice of times for the interview, being respectful of his or her workload.
- iii. Provide the subject with a rough estimate of the amount of time the interview will take.
- iv. Remove extra distractions, such as computers, files, paperwork, in the interview room.
- v. Provide the interviewee with a comfortable chair that doesn't face a window.
- vi. Create a comprehensive list of investigation interview questions that you can choose from, depending on the direction the interview takes.
- vii. Decide whether or not to record the investigation interview.
- viii. Put the subject at ease when he or she arrives and offer a glass of water or coffee.

Questions

Begin by establishing a baseline by asking simple, easy-to-answer questions that the subject is likely to answer truthfully, such as: How long have you worked at the company?

- i. Ask open-ended questions to get the subject to talk, such as: Tell me about...
- ii. Avoid loaded questions, such as: Are you a tough supervisor?
- iii. Avoid questions at the beginning that can be answered with a yes or no.
- iv. Do not ask accusatory questions that indicate you think the subject is guilty.
- v. Ask simple questions that address one fact at a time, rather than combining more than one idea into the same question.
- vi. Do not ask leading questions that prompt for the answer you want, such as: Isn't it true that you punched Jean?
- vii. Ask yes or no questions at the end of the interview to pin down specific facts that were revealed during the interview.

Objectivity

- i. Explain that you are taking every allegation seriously and are committed to finding the truth.
- ii. Ask the subject to keep the interview confidential only if you have already established grounds for confidentiality.
- iii. Don't promise confidentiality but tell the subject that you will share information with only those who need to know.

- iv. Avoid being too familiar or taking on the role of “one of the guys”.
- v. Do not share information about what other interview subjects have said (unless you are interviewing the accused or trying to obtain information from a hostile witness).
- vi. Avoid expressing your thoughts, opinions, or conclusions about the case or what the interviewee says.
- vii. Do not make agreements or deals with the subject.
- viii. Practice self-awareness by identifying your own potential biases and putting them aside while conducting the interview.

Development

If the interview is about a specific event, identify the five Ws: who, what, when, where, why.

- i. If the interview is about a specific event, identify the five Ws: who, what, when, where, why.
- ii. Proceed in chronological order to ensure nothing is missed.
- iii. Ask about witnesses or others who can corroborate or comment on the incident.
- iv. Ask the subject to recreate the dialogue of the incident, in order of what was said.
- v. Request any notes, documents, phone messages, or other evidence.
- vi. Identify the source of the subject’s knowledge: hearsay, rumor, eyewitness, other direct knowledge
- vii. Take detailed notes (or have another person present who is taking detailed notes) that list only what is revealed in the interview, without opinion or comments.
- viii. Note the subject’s body language and physical movements, but without interpretation. For example, write that the subject was tapping his foot rapidly, but not that the subject seemed nervous.

Summary

- i. Repeat any questionable or confusing information back to the subject to ensure you heard correctly.
- ii. Get the witness to confirm any areas where you may have misheard or misinterpreted information.
- iii. Ask for clarification and more detail on any vague points.
- iv. Ask follow-up questions to establish more facts in the chain of events, for example: If you were in the cafeteria at 1pm, how did your access card register an entry into the library at the same time?

- v. If the subject gave evasive answers or avoided a question, rephrase the question and ask it again.
- vi. Ask the subject whether there are any other questions they feel you should have asked or whether there is anything they would like to disclose before you conclude the interview.
- vii. Allow sufficient time for the subject to think before answering any final questions.
- viii. Use silence as a tool to prompt a reaction, when possible.

Building Rapport in Investigation Interviews

Investigators who build rapport with interview subjects develop trust and credibility and are able to get better information from interviews. Two important skills investigators can use to build rapport are mirroring and developing shared experiences.

Mirroring

Subjects in investigation interviews are more likely to identify with and trust people who are like them. Investigators can encourage this through mirroring, a technique that involves a subtle method of shared rhythm, matching language, and tone of voice and assuming similar body positions as the subject. The following three tips can help investigators to mirror successfully:

- Learn as much as you can about the interviewee. Investigators must understand the emotive state of each interviewee to mirror them successfully. Conduct background research on the interviewee's culture, habits, hobbies, and attitudes before the interview.
- Don't mimic or mock. Be similar to the person you are interviewing without making it obvious. Don't copy their movements too quickly. Be as subtle as possible to avoid detection, which would likely offend the subject and jeopardize your chance of getting the truth.
- Proceed slowly. If someone appears closed at the outset of the interview, mirror the closed demeanour and slowly begin to open up. Often, the subject will see that you are more relaxed and will begin opening up as well.

Some Additional Tips:

- Dress in a similar style and level of formality as the interviewee.

- Sit at the same level as the subject.
- Listen actively by maintaining eye contact and making encouraging sounds.
- Be aware that the interviewee may be nervous or unwilling to cooperate with you.

Developing Shared Experiences

Developing shared experiences allows the interviewee to identify with the interviewer. A brief discussion about a common interest or experience – sports, weather, traffic, etc., can help open the doors to a conversation and relax the interviewee.

- Get a conversation going. Ease into interviews by asking subjects about themselves, their jobs and outside interests.
- Ask follow-up questions and demonstrate a genuine interest in what the interviewee has to say. Use the interviewee's name during the conversation and, most importantly, let the subject do the talking.
- Establish a baseline. Pay attention to the interviewee's tone of voice, pace of speech and physical movements (or lack of) during the initial, rapport-building conversation. This allows an investigator to establish a baseline of speech and behaviour that can be used to evaluate future responses, as some people change the way they speak or act when they aren't being honest.

Maintaining Rapport

In order to maintain rapport with the interviewee, an investigator needs to be flexible and reactive, and may need to make subtle adjustments throughout the interview, based on the subject's responses and behaviour. Should the interviewee start to become closed off as the interview progresses, the techniques of mirroring and shared experiences can be used to get a subject to open up again.

Investigation Interview Questions for the Complainant, Subject and Witnesses

Take your investigation interviews beyond the who, what, where, when, why and how of what happened. Knowing what questions to ask in an investigation interview comes with experience. Investigators who have interviewed thousands of complainants, witnesses and subjects know the standard questions they should always ask, but they also know the importance of following the trail to ask new questions based on the information revealed.

Therefore, while the investigation interview questions below provide a great basis for starting the conversation and covering the basics of what happened, don't limit yourself. It's by asking the probing questions that arise from what's revealed in the conversation that the whole truth is uncovered.

Questioning the Complainant

It's important to take the reporter's complaint seriously, no matter how frivolous it may seem at first glance. There have been cases of reports of minor infractions that, under investigation, revealed much larger issues.

Another reason to take complaints seriously is to assure the complainant and others that the AOG will follow up and provide a fair assessment of their concerns, no matter how small. This helps to establish a speak-up culture and increases the chances that people will come forward in the future. The complainant is usually the first person interviewed in an investigation.

Sample Questions to Ask the Complainant:

Here are 16 sample investigation interview questions to ask the complainant:

- i. What happened?
- ii. What was the date, time and duration of the incident or behavior?
- iii. How many times did this happen?
- iv. Where did it happen?
- v. How did it happen?
- vi. Did anyone else see it happen? Who? What did they say? What did they do?
- vii. Was there physical contact? Describe it. Demonstrate it.
- viii. What did you do in response to the incident or behaviour?
- ix. What did you say in response to the incident or behaviour?
- x. How did the subject of the allegation react to your response?
- xi. Did you report this to anyone in management? To whom? When? What they say and/or do?
- xii. Did you tell anyone about the incident or behaviour? Who? What did they say and/or do?
- xiii. Do you know whether the subject of the allegation has been involved in any other incidents?

- xiv. Do you know why the incident or behaviour occurred?
- xv. Do you know anyone else who can shed light on this incident?
- xvi. Is there anything else you want to tell me that I haven't asked you?

Questioning Witnesses

After questioning the person who filed the complaint, the next step is to interview any witnesses to the incident being reported. Witnesses can help to corroborate or refute the reporter's account of what happened and shed light on some of the details that the reporter may not have been able or willing to furnish.

The most compelling witnesses are, of course, those who actually witnessed the incident. But witnesses can also be those who heard about the incident from others who witnessed it or those to whom the reporter relayed the incident after the fact. It can also be helpful to interview witnesses to other incidents that the subject of the complaint was involved in.

Sample Questions to Ask the Witnesses:

These 14 sample investigation interview questions can help get witnesses to talk:

- i. What did you witness?
- ii. What was the date, time and duration of the incident or behavior you witnessed?
- iii. Where did it happen?
- iv. Who was involved?
- v. What did each person do and say?
- vi. Did anyone else see it happen? Who?
- vii. What did you do after witnessing the incident or behaviour?
- viii. Did you say anything to the parties involved in response to what you witnessed?
- ix. How did the complainant and the subject of the allegation react to your response?
- x. Did you report this to anyone in management? To whom? When? What they say and/or do?
- xi. Did you tell anyone about the incident or behaviour? Who?
- xii. Do you know why the incident or behaviour occurred?
- xiii. Do you know anyone else who can shed light on this incident?
- xiv. Is there anything else you want to tell me that I haven't asked you?

Questioning the “Accused”

Keeping in mind that the purpose of interviewing the subject of the complaint (also known as the accused) is simply to find out the truth, it’s important to pay attention to credibility clues and be aware of any biases that may affect your judgment. Questioning the accused person is often the most sensitive of all the interviews you will conduct. You’ve heard the accounts of everyone else involved in the incident, and it’s difficult to avoid forming an opinion before getting to this crucial interview. But it’s important that you keep an open mind to avoid making assumptions based on what you’ve already heard.

Sample Questions to Ask the Subject of the Complaint:

Here’s what to ask the subject of the complaint:

- i. What happened?
- ii. If the subject denies that the incident occurred, ask:
- iii. Is there any reason anyone would invent or lie about the incident?
- iv. Where were you when the alleged incident occurred?
- v. Do you have any witnesses who can corroborate your whereabouts at the time of the incident?
- vi. If the subject doesn’t deny that the incident occurred, ask:
- vii. When and where did this happen?
- viii. What were the circumstances leading up to the incident?
- ix. Who else was involved?
- x. What is your connection to the complainant?
- xi. Are you aware of any other complaints by this person?
- xii. Recount the dialogue that occurred in order of what was said.
- xiii. What did the complainant do or say?
- xiv. Is there any evidence to support your account of what happened?
- xv. Is there anyone else we should talk to who had knowledge of the incident or the circumstances surrounding it?
- xvi. Have you talked to anyone about the incident? Who? What did you tell them?

Tips for Questioning All Parties

The most important thing to remember when conducting investigation interviews is that your main objective is to simply find out the truth about what happened. There will be

barriers, detours, and challenges along the way, but as long as you stay focused on that one goal, you'll stay on track.

One of the challenges you'll face is staying objective. Everyone has personal biases and it's an investigator's job to recognize those biases and take them into account. This takes a great deal of self-awareness and self-control, but an excellent investigator has both qualities.

When assessing the creditability of the subject, complainant, and witnesses, you'll also need to keep your biases in check and follow best practices. Before beginning the questioning phase above, ask some basic questions that are not connected with the incident being investigated. They should be non-threatening questions to which you already know the answers. This helps you to establish a baseline against which you can measure the person's subsequent behavior, language, and manner.

Baseline Questions

Examples of baseline questions are:

- How long have you worked at the company?
- What is your position?
- How long have you been in this position?

Notice the interviewee's speech patterns, gestures and degree of eye contact when answering these non-threatening questions. This helps you to assess whether there are differences in their behaviour when you ask questions related to the incident.

Recording an Interview

Investigators are strongly advised to recording the interview whether by audio or video as this has numerous critical advantages. It permits the interviewer to concentrate more effectively on the suspect's account and to encourage disclosure; and comprises a verbatim electronic record of what was said which cannot be disputed. In addition, the recording itself can afterward be replayed and reviewed by investigators and may help identify points that were missed within the interview which needed to be followed up.

Chapter 15: Investigative Report Writing

An investigation report documents in detail the findings of an investigation. This is where investigators record the substantive issues, analyze the evidence, formulate a conclusion, and make recommendations for next steps. The process of writing the investigation report can sometimes clarify your thinking and can even uncover additional questions that provide new insight into a case. The investigation report also provides valuable data that can be used to implement control and preventive measures in your organization.

Writing an investigative report is one of the most tedious tasks an investigator undertakes. The investigative report reflects on you, the investigating team and the quality of the investigation. Therefore, make sure it's skillfully written, clear and comprehensive, and is as accurate as possible.

An investigative report has many purposes.

- It's the document that ignites action based on the official findings it presents. This could be a termination of employment, corrective action, implementation of training, or some other action taken based on the findings.
- The investigation report is also a record of the steps of the investigation. It can be used to prove that your investigation was timely, complete, objective and fair.
- The information contained in the investigation report may be cited in legal action, so it's important that the report is detailed and accurate but does not include unnecessary or irrelevant detail which may cause difficulty.
- Finally, the investigation report provides valuable data that can be used to implement control and preventive measures.

Investigative Report “Musts”

Before writing the report, it's important to understand the three critical tasks of an investigative report.

- It must be organized in a way that anybody internally or externally can understand it without having to reference other materials.
- It must document the investigative findings objectively and accurately and provide decision makers with enough information to determine whether they should take further action.

- It must indicate whether the allegations were substantiated, unsubstantiated or whether there's something missing that is needed to come to a conclusion.

Steps on How to Write an Investigation Report

Introduction & Overview –

- How and when the problem or complaint arose and when it came to the employer's attention. The names and titles of the investigation(s). Summary of investigation process used. When the investigation began and was completed.

Executive Summary

- The Executive summary helps high-level stakeholders get an overall picture of the allegations, investigation, and outcome.
- The Executive summary should be a concise overview of the investigation from beginning to end. It should not contain any information that is not already in the investigation report. Write in an active voice.

- **Retention Of Investigation Reports**

- Retain ALL investigation materials
- Do not discard drafts or working notes.
- Keep an organized file.
- Date your interview notes
- Keep a chronology
- Keep in confidential and secure location
- Evidentiary sanctions are possible for willful destruction of investigative materials
- Be familiar with your organization or client's retention policies

- **Summary Of Allegations & Factual Findings**

- **Use** – a separate heading for each allegation followed by the response or summarize all allegations and then summarize response and other factual findings
- **Consider** – including chronology of events

- **Highlight** – any factual discrepancies

- **Conclusions** – Primary questions to answer: Was there financial misconduct or not?
 - Apply policies to the facts
 - Decisions-maker cannot make use of the report if there are conclusions but no explanations for the conclusions.
 - If there is litigation, investigator will be expected to be able to articulate reasons for conclusions.
 - Identify any issues that could not be resolved during the investigation and state why.

- **Documenting Credibility Decisions** – If a credibility decision has to be made, explain the basis for it (how and why one person or description of events was more credible than another)
 - In most cases, there will be some corroborating evidence
 - If the investigator absolutely cannot make credibility call, say so. For example: Both parties were credible in their statements and explanations for their actions. There is no evidence to support fabrication of the claim, yet no other evidence to support that the actions occurred. There are no eyewitnesses to the conduct, and the accused has denied engaging in the actions.

- **Document the Evidence**

In this section, describe all the evidence obtained. This could include video footage, email records, employee security access records, computer login records, documents or papers, physical objects, etc. Number the evidence and refer to any physical evidence by the number recorded on the chain of evidence document.

It's critically important to include and fully consider **all** evidence obtained, whether or not it supports your position. Ignoring evidence that doesn't support your conclusion will undermine your investigation and your credibility as an investigator. As long as you have a good explanation of why certain evidence is not being weighted as heavily as other evidence, your conclusion is defensible.

- **Recommendations For Corrective Action**
 - Determine if corrective action is required

- If no violation occurred, no corrective action is needed
 - If a violation occurred, corrective action recommendations should be designed to prevent any future occurrences of similar conduct to mitigate legal risk
 - Some organizations may desire recommendations for remedies for issues that are still problematic, even if they do not rise to the level of a violation.
 - Some organizations will ask that the investigator include recommendations for corrective action in the written report only after the report and conclusions have been reviewed by management
 - Best practice is to include what remedy was implemented and when – often as addendum to report.
- **Avoiding Pitfalls**
 - Make findings that relate to the evidence: not conclusions of law
 - You are investigating whether there is evidence to suggest unlawful misconduct, not a violation of the law
 - Only a judge or jury decides whether there has been a violation of law, and only if lawsuit is filed
 - Only make findings of fact and provide the facts that support the conclusion reached
 - Be watchful for typos and errors – this is not just about professionalism, it's about credibility for e.g. spelling, grammar , quotations , punctuation, abbreviations, tenses, tone/style, redundancy
- **Communication The Report to Management And/or Third Parties**
 - Determine if draft report needs legal review prior to finalizing
 - Discuss and resolve any privilege issues with legal counsel regarding distribution of report
 - Consider whether verbal summary update prior to written report is advisable
 - Report does not go to complainant or accused - shared with management on need-to-know basis only
 - Ensure final copy is version provided to government agency/discovery process

- **Check Your Work**

Keep in mind that your investigative report may be seen by your supervisors, as well as attorneys and judges if the case goes to court.

If you're not a stellar grammarian, if your spelling leaves something to be desired and if your punctuation is less than perfect, you may want to enlist the services of a writer-friend or colleague to proofread your investigative report. Or, if you're a lone wolf kind of worker, upgrade your skills. And always remember to run a spell check before you pass on any document to others.