



## OECD International Academy for Tax Crime Investigation

*Managing Financial Investigations*

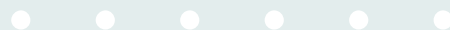


# Financial Intelligence & Sources of FI

Olivia Okello, CPA(K)

March, 2024

GDF, Ostia, Italy





# Financial Investigations

---

- A financial investigation is an analysis of:-
  - Source of the money
  - Movement of money , and
  - Its use
- A key component of financial investigations is the determination of the financial gain or profit derived from the predicate offence.
- Requires the use of a variety of investigative techniques to trace assets, analyze financial data and gather financial information



# Financial Investigations

---

Most Investigators struggle with;

- What to look for,
- How to structure the data obtained,
- How to analyze data and information,
- How to present information and evidence for use in court,
- Fail to anticipate the defenses that can be raised by the suspect - think like the suspect.



# Financial Investigations

---

- Encounter Accounting & Financial systems unfamiliar to investigators,
- Have Budgetary restrictions – equipment and tools
- Do not understand the full scope of legal issues
- Lack adequate human resources – Numbers and Expertise, complex investigations
- Have a silo mentality





*What is the role of Financial Intelligence  
in any investigative process?*



# Financial Intelligence?

---

- Financial Literacy???
- Serves to increase a decision-maker's certainty and awareness
- Helps to understand Financial Crime Risk Indicators and Risk Management
- Facilitates successful Financial Fraud Investigations
- Roles in Intelligence Management – Collection & Analysis



# Tax crime intelligence

---

Tax Intelligence is;

*The systematic use of:*

- *Specialized techniques, aimed at the production of information, for the purpose of assisting the tax administration in the planning and execution of its legal functions, including revenue collection, combatting tax evasion and financial crimes.\**

*Source: \*Inter American Center of Tax Administration - CIAT*





# Tax crime intelligence

---

- **Tax crime intelligence** refers to information gathered or collated, analyzed, recorded/reported and disseminated by tax authorities concerning types of tax crimes, identified criminals and known or suspected criminal groups.
- The aim of tax intelligence gathering is to **obtain, analyze and sharing knowledge** about events and situations which may have an immediate or potential influence on tax compliance.



# Intelligence Vs Evidence

---

- The process of intelligence gathering in relation to a specific investigation is usually a prelude to any evidence gathering phase.
- A state's national legislation will dictate the way intelligence can be used for law enforcement purposes.
- Legislation will also dictate whether intelligence material gathered during the course of an investigation is protected from disclosure in criminal proceedings

# Types of Intelligence

- ***Strategic intelligence:***

- Focuses on the long-term aims of law enforcement agencies.
- Reviews current and emerging trends, changes in the crime environment, threats to public safety and order,
- Considers opportunities for controlling action and counter programmes,
- Comes up with change to policies, programmes and legislation.

- ***Operational intelligence:***

- Provides hypotheses and inferences concerning specific criminal networks, individuals or groups involved in unlawful activities,
- Discusses their methods, capabilities, vulnerabilities, limitations and intentions that could be used for effective law enforcement action.

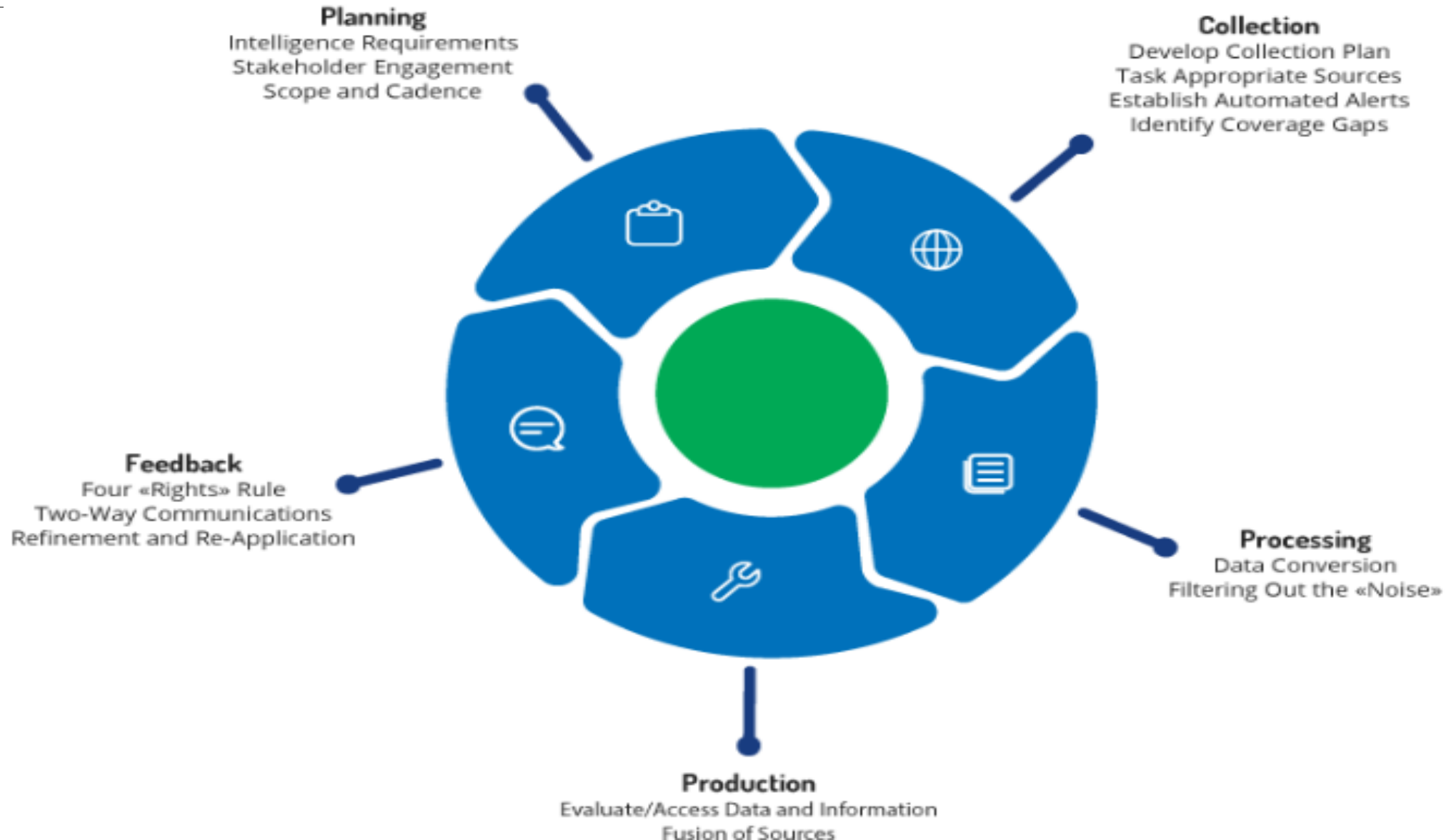
# Proactive Vs Reactive Intelligence

- **Pro-active tax intelligence** refers to the activity of obtaining and analyzing the information, with the aim of combating tax and customs violations, as well as the improvement of the tax legislation or administrative procedures.
- **Deterrence.**

- **Reactive tax intelligence** assumes the form of investigation, helping the gathering of evidence and leads that can be used for administrative purposes and for instructing the criminal recourse.
- **Detection and Disruption.**



# INTELLIGENCE CYCLE



# Intelligence Cycle



## Planning

- Consider the Investigations' needs
- Tasking
  - Who tasks?
  - How do they task?
  - Why do they task?
  - What tasks are set?



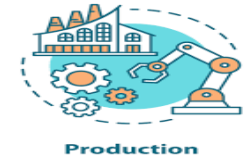
## Collection

- Refers to process to obtain and use of data
- **Collection plan:** a formally defined approach to describing the Information needed and means of acquiring it



## Processing

- Collation
- Integration & Analysis
- examination of the information to make meaning.
- Inferences
  - Hypothesis
  - Prediction
  - Estimation
  - Conclusion

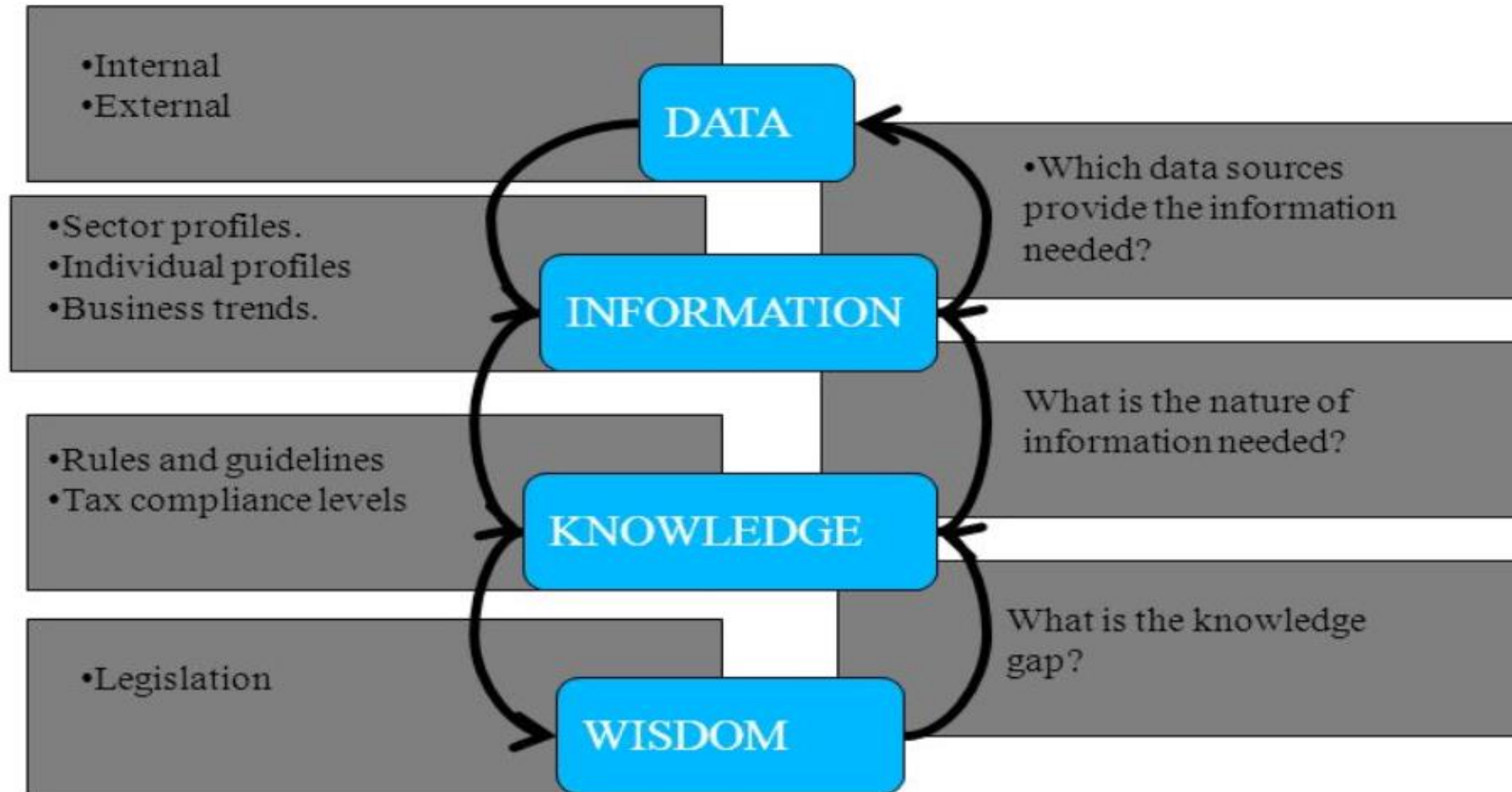


## Production & Dissemination

- Preparation of Output
- Formats
  - Structured formalized report
  - formal oral presentation
  - Bulletins
  - Ad-hoc briefings - operational



# Intelligence Life Cycle





# Intelligence Collection Disciplines

---

- i. **Human Intelligence (HUMINT)** is the collection of information from human sources
- ii. **Open-Source Intelligence (OSINT)** refers to a broad array of information and sources that are generally available
- iii. **Signals Intelligence (SIGINT)** refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites.
- iv. **Imagery Intelligence (IMINT)** is sometimes also referred to as photo intelligence (PHOTINT).
- v. **Measurement and Signatures Intelligence (MASINT)** is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities.





# Sources Of Information



# Classification of Intelligence Sources

---

- Influenced by need or not to use Intelligence specialized techniques for their collection.
- Mainly qualified as:
  - **Open sources** (grey literature) is information that is publicly available
  - **Closed source** is information collected for a specific purpose with limited access and availability to the general public e.g. Govt. Databases
  - **Classified** is information collected by specifically tasked covert means including use of human and technical resources. Very accurate but may be un actionable due to imposed restrictions



# Sources of Financial Information

---

- ◎ Bank Records - Core financial i.e. statements, deposit and withdrawal records, loan records, and records of checks.
- ◎ Wire transfer records - electronic fund transfers, domestic or international.
- ◎ Investment Accounts - Brokerage statements, transaction records, and holdings information pertaining to stocks, bonds, mutual funds, or other investments.
- ◎ Credit Card Records - Statements and transaction details offer insights into spending patterns, revealing unusual purchases that could be linked to criminal activity or used to launder money



# Sources of Financial Information

---

- ◉ Financial Records - Financial statements, invoices, contracts, tax records, and internal documents specific to a business involved in the suspected activity.
- ◉ Block chain Analytics - Block chain technology, with its public ledger system, can be used to trace the movement of crypto assets, identify suspicious wallets.
- ◉ 3<sup>rd</sup> Party data providers - Specialized firms offer access to comprehensive data sets, including consumer spending, business ownership structures, and financial transactions.



# Sources of Financial Information

---

- ◉ Financial Disclosures - Reports required for (PEPs) or disclosures associated with certain financial transactions. These offer information on significant holdings and potential sources of unexplained wealth.
- ◉ Digital Evidence Sources - Emails, text messages, computer files, and data from websites or social media relevant to the suspected crime. These contain communications and potential evidence of coordination between perpetrators or admissions of guilt.



# Group Discussion

---

- i. Group 1 - Tax Administration
- ii. Group 2 – Public Prosecutor
- iii. Group 3 – Anti Corruption Agency
- iv. Group 4 - Asset Recovery Agency



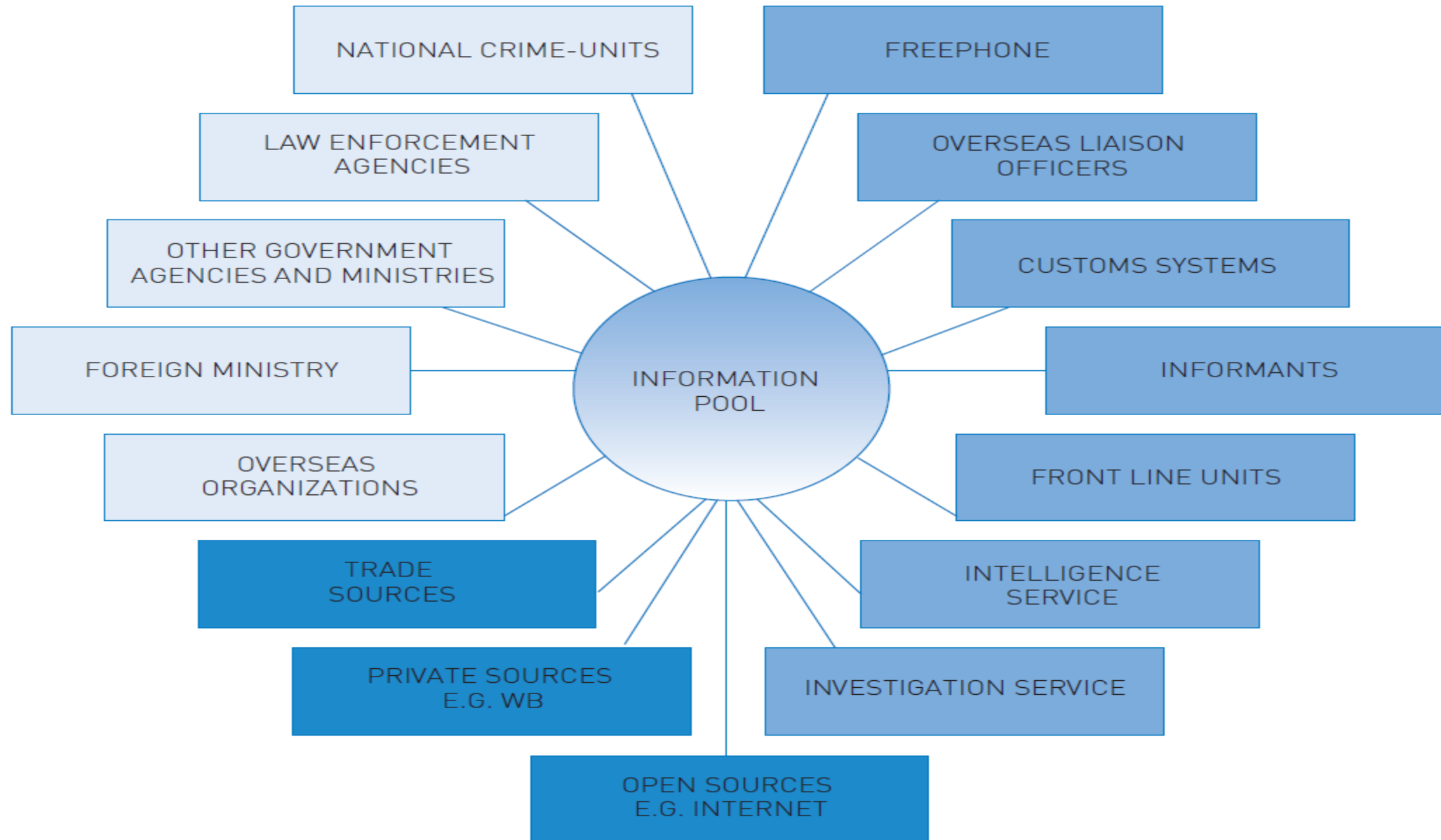
# Group Discussion

---

- i. Which data sources does your organization rely on when conducting its audits and/or investigations? List both Financial and Non Financial Data Sources.
- ii. How do you acquire this information/which tools do you use?
- iii. What other data/information sources are known to you as an agency but are not optimally utilized?
- iv. In reference to your answers in (i) and (iii) above, why aren't you using all the data sources known to you? Challenges?
- v. Suggested Remedies/Recommendations



# Information Pool







# 1. Internal Sources

---

- Structured, Sensitive and regulated.
- Decisions to be made about which data is important to an organization and the format/nature of data.
- Data to be audited regularly as it could be outdated or even illegal due to changing regulatory frameworks.



# 1. Internal Sources

---

- Organization's databases e.g. Tax Fillings, Registrars
- Self Declarations/Self Fillings e.g. wealth declarations for public officers.
- Considerations:
  - Information Integrity – Accuracy/Relevance
  - Information Security – Reliability
  - Data Mining - Ease of Access, Methods of access
  - How intelligent is your data?



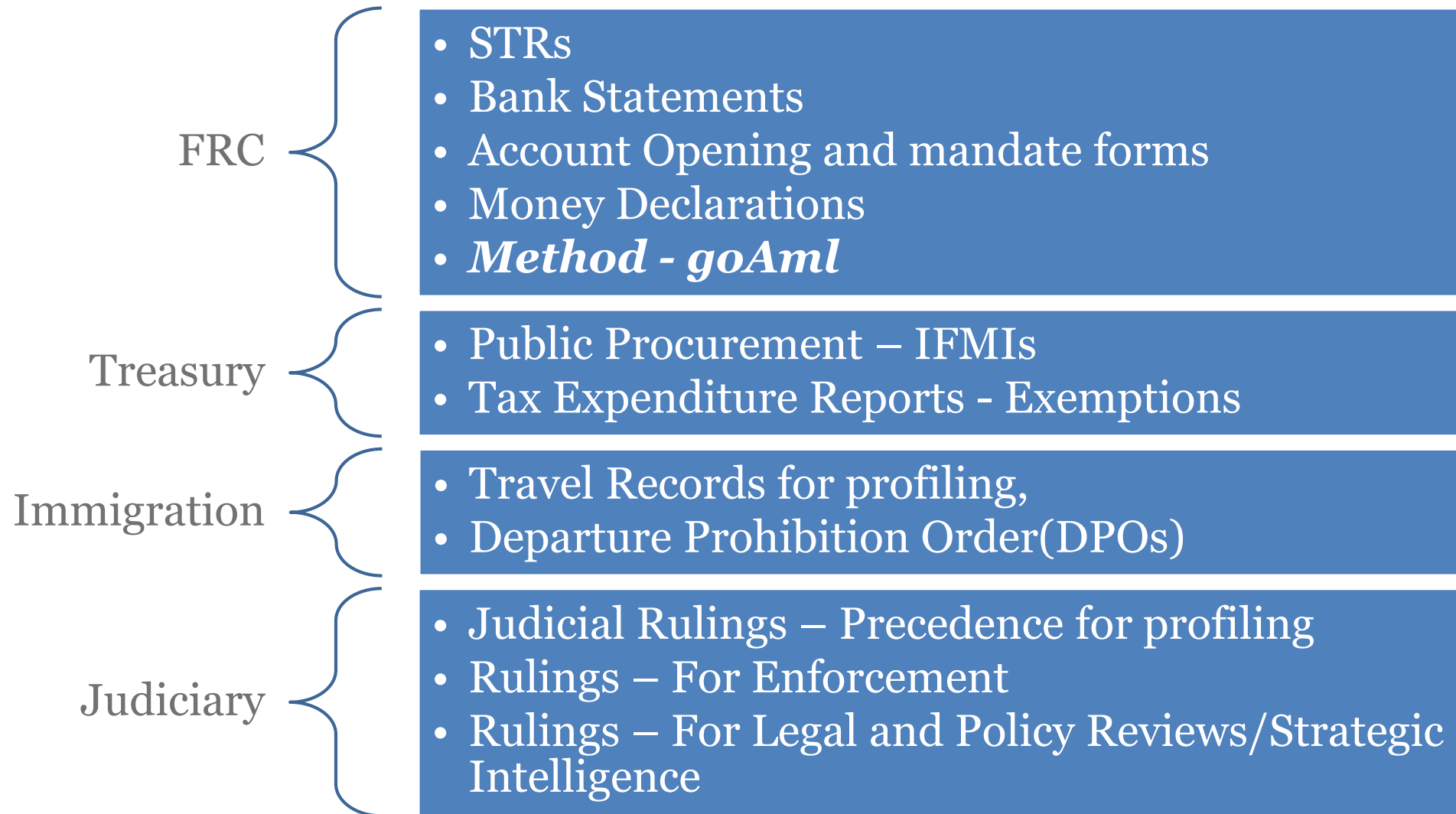
## 2. Inter Agency Sources

---

- Legal Tools
  - Legislation
  - MOUs
  - TORs
- Methods/Process Gateways Must Exist!!!
  - Direct access to information contained in agency records or databases;
  - an obligation to provide information spontaneously (sometimes expressed as a “reporting obligation”
  - an ability, but not an obligation, to provide information spontaneously; and
  - an obligation or ability to provide information only on request



## 2. Inter Agency Sources





## 2. Inter Agency Sources

Registrar of  
Companies

- Directors Details
- Related/Associated Companies
- Beneficial Ownership
- Company Structures

Utility Service  
Providers

- GEO coordinates
- No. of Properties
- Ownership Details

Registrar of  
Motor Vehicles

- Ownership Details
- Financed/Attached
- YOFR/Acquisition
- Motor Vehicle Transfers

NPS/DCI

- Subject Details – Case specific, upon request



# FIU/FRC

---

- Is a central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to the competent authorities.
- Scope of responsibilities is defined national legislations and differ from jurisdictions.
- Financial Action Taskforce (FATF) s an inter-governmental body which sets standards, and develops and promotes policies to protect the global financial system.
- Provides 40 recommendations, For FIUs, refer to Recommendations 26 -32.



# United Nations Convention against Transnational Organized Crime

*Palermo, December 2000*

## *Article 7. Measures to combat money - laundering*

- Shall[...]ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money laundering (including, where appropriate under domestic law, judicial authorities) **have the ability to cooperate and exchange information** at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a **financial intelligence unit** to serve as a national centre for the **collection, analysis and dissemination of information** regarding potential money laundering.
- States/Parties shall consider implementing feasible measures to **detect and monitor the movement of cash** and appropriate negotiable instruments across their borders, subject to safeguards to ensure proper use of information and without impeding in any way the movement of legitimate capital. Such measures may- include a requirement that individuals and businesses **report the cross –border transfer of substantial quantities of cash** and appropriate negotiable instruments.



# Egmont Group

---

- ◉ Established in 1995 as an informal group to facilitate cooperation in the areas of information exchange, training and the sharing of expertise.
- ◉ Members – 166 out of 195 countries globally
- ◉ Africa falls under 3 regions – Middle East and North Africa(14), East and South Africa(10) and West & Central Africa(14)





# Financial Intelligence Units - Scope

---

## Cash Transaction Reports (CTR)

CTR refers to all reports of cash transactions

## Suspicious Transaction Reports (STR)

STRs can be uploaded or created manually

## Cross-Border Reports

Transactions that involve sending or receiving money across borders.

## Unusual Transaction Reports (UTR)


UTR relates to all unusual (cash) transactions that might be suspicious. After examination, a UTR can be dismissed as unsuspicious or raised to an STR.

## International Funds Transfer (IFT)

IFTs are transactions in which money is sent to from one country to another.

## Additional Information File (AIF)

AIFs are replies to requests for information when the analysts require more details on transactions, involved persons, accounts, or entities.





# Functions of the FRC - Kenya

---

- ✓ *An independent body whose principal objective is to identify proceeds of crime and money laundering and whose functions include;*
  - i. Receipt and Analysis of STRs by Reporting Entities
  - ii. Receipt and Analysis of Cash Declarations at Points of Entry.
  - iii. Dissemination of Reports received under the Act to appropriate law enforcement authorities
  - iv. Inspection and Supervision of Reporting institutions for Compliance with AML/CFT obligations
  - v. AML/CFT training and capacity building
  - vi. Facilitating EOI on money laundering with other FIUs in other countries.



# Requesting information from an FIU

---

© Requesting financial information from an FIU involves the following steps:

**Step 1.** A domestic agency (i.e., a financial supervisor or law-enforcement agency) or a foreign FIU makes a request for financial information to support a case involving money laundering, terrorist financing, or related crimes.

**Step 2.** The requested FIU determines whether the request satisfies legal, policy, and operational requirements. If so, the FIU searches its databases and files for information responsive to the request.

**Step 3.** If necessary and appropriate, the FIU seeks information from other government agencies and financial institutions to respond to the request.

**Step 4.** The FIU analyzes the information and prepares a report to share with the requesting agency or FIU and determines the conditions under which the requesting agency or FIU may use and disseminate the information contained in the report.

© [https://goaml.frc.go.ke/goAML\\_Prod/Home](https://goaml.frc.go.ke/goAML_Prod/Home)



### 3. Open Sources

---

- ◉ Intelligence from publicly available sources—*open* refers to “overt”
- ◉ It has been estimated that roughly 90% of valuable intelligence comes from **open sources**
- ◉ According to the CIA, open sources often equal or surpass classified information in monitoring and analyzing issues including terrorism, proliferation, and counterintelligence...



### 3. Open Sources

---

- ◉ ***As an investigator, Consider;***
  - Who has jurisdiction?? – Access and Admissibility
  - Open source Information is not secure and be easily lost or corrupted – Preservation and COC
  - Investigations vary in scope and complexity – Skills??
  - Where to begin?? – TMI
- ◉ Sample Open Sources include:
  - [https://i-intelligence.eu/uploads/public-documents/OSINT\\_Handbook\\_2020.pdf](https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf)



## 4. International Sources - Legislation

---

- ◉ Various legal instruments are available to investigators to facilitate international cooperation.
- ◉ Start point - Enabling Domestic Legislation
- ◉ Sample Specific Instruments include;
  - ◉ <https://www.oecd.org/corruption-integrity/checklists/international-co-operation-fight-against-financial-crimes-available-instruments-aci.html>



# Financial Intelligence Networks

---

National  
Networks

Regional  
Networks

International  
Networks



# International Sources - Networks

---

Broadly, information can be obtained through formal and informal inquiries

- **Global Networks e.g.** Interpol, EGMONT Group
- **Regional Networks e.g.** Europol, Afripol, ARINSA
- **National Networks e.g.** FIUs, Law enforcement collaborations
- **Public-Private Partnerships e.g.** Joint Money Laundering Intelligence Taskforce (JMLIT)
- **Intelligence sources e.g.** RILO, Intelligence Community(USA)

NB: Asset Recovery Networks:

<https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2018-June-6-7/V1803851e.pdf>





# Social Media Investigations

---

- ◉ Has become a standard requirement for most investigations e.g. Insurance Fraud, IP theft, Online Defamation and Criminal Proceedings.
- ◉ You will often get both Financial indicators and/or Circumstantial evidence from social media.
- ◉ Challenge is how? A number of social media investigations tools are available, some free and some paid;



# Investigative Issues

---

Criminals may use the Internet for numerous reasons including:

- Trading and sharing information such as IDs, photos, tickets, financial data, etc.
- Display of lifestyle – trophy cabinets
- Concealing their identity
- Identifying and gathering information on victims
- Communicating with co-conspirators
- Distributing information
- Coordinating meetings, parcel drops, etc.



# Social Media Investigations Tools

---

- **WebPreserver:** Collect and preserve social media evidence in defensible format - <https://www.pagefreezer.com/webpreserver/>
- **Makeawebsitehub:** Identify the latest social media apps and platforms
- **Pipl Search:** Find public records, online data, and other information related to an individual - <https://pipl.com/>
- **TinEye:** Use reverse image search to find the source of an online picture
- **TweetBeaver:** Use Twitter analytics to understand an account and identify connections



# Documenting OSINT Intelligence

---

- Record URL's e.g. Web preserver
- Email communications (keep copies of relevant correspondence)
- Screen capture – Print screen, Save As or apps such as 'Camtasia' or 'HTTrack'
- Depending on nature of case keep hard copies of screen shots, emails etc...



# Pitfalls of Investigating on the Internet

---

All enquiries will leave a footprint!

- Devices will leave footprints across the internet
- Disguise your online ID (Proxy and VPN services reroute your internet traffic and change your IP)

Consideration must be given to the type of investigation being undertaken and the risk of compromise.

- Open source carries greater risk
- Digital evidence is fragile and can be easily lost or corrupted

Secure way of browsing

- Secure your browsers –as simple as an update!
- Do not be tempted to use your own devices!
- Try; [fakenamegenerator.com](http://fakenamegenerator.com), [torproject.org](http://torproject.org)

Integrity of the investigation

Personal security





# Google Cache and Privacy

---

- Web browsers are designed to download Web pages and store them locally on your computer's hard drive in an area called cache
- Browser cache (also known as Internet cache) contains records of every item you have viewed or downloaded whilst surfing the Internet
- When you visit the same page for a second time, your browser speeds up display time by loading the page locally from cache instead of downloading everything again.
- Internet cache can pose a threat to your privacy as everyone who has access to your computer can see some personal information by simply opening the cache folder
- In most browsers, you can clear the cache from the Privacy or History area in the Settings or Options menu, depending on the browser



# Feedback Session