Designing a tax crime investigation manual

Key elements and considerations

Designing a tax crime investigation manual

Key elements and considerations

This work was approved and declassified by the OECD Committee on Fiscal Affairs on 4 May 2025.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Note by Türkiye:

The information in this document with reference to "Cyprus" relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Türkiye recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Türkiye shall preserve its position concerning the "Cyprus issue".

Note by all the European Union Member States of the OECD and the European Union:

The Republic of Cyprus is recognised by all members of the United Nations with the exception of Türkiye. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

Please cite this publication as:
OECD (2025), *Designing a tax crime investigation manual: Key elements and considerations,* OECD Publishing, Paris, https://doi.org/10.1787/f2870e23-en.

Photo credits: © 2017 Gorodenkoff/Shutterstock

Corrigenda to OECD publications may be found at: https://www.oecd.org/en/publications/support/corrigenda.html.

Preface

As tax crimes become more sophisticated, jurisdictions must strengthen their investigative capabilities to protect public revenue and maintain trust in the tax system. The Task Force on Tax Crimes and Other Financial Crimes (TFTC)'s guide on Designing a Tax Crime Investigation Manual is a vital resource that will serve as an indispensable guide for tax investigators and professionals. This effort also highlights the invaluable work done by TFTC in empowering jurisdictions with the tools and knowledge needed to tackle the complexities of tax crime detection and investigation.

Tax crime is a global issue, and without a structured approach, jurisdictions risk missing opportunities to detect investigate and prevent fraudulent activities that undermine the integrity of their tax systems.

The weaknesses in one jurisdiction can create vulnerabilities for the entire global system. Furthermore, the absence of standardised investigative frameworks has often hindered the effectiveness of tax crime investigations. This manual will serve as a crucial tool to bridge these gaps, providing a comprehensive set of guidelines that will empower investigation teams to conduct thorough and consistent investigations.

In 2024, as part of its involvement in the joint OECD-UNDP Tax Inspector's Without Borders Criminal Investigation Programme, the Maldives Inland Revenue Authority launched its first domestic tax crime investigation manual with the invaluable support from our counterparts at the Australian Taxation Office We are proud that our country's investigation manual has inspired and contributed to the development of this global guide that will support other jurisdictions' approach to domestic tax crime investigations. Strong partnerships and sharing of knowledge between jurisdictions are essential in tackling tax evasion, fraud, and other financial crimes. By learning from each other's experiences, we strengthen our collective efforts to combat illicit financial activity.

We are proud to have collaborated with TFTC in this endeavor. I commend the efforts of all those involved in the development of this Guide, and I am confident that it will play a crucial role in the global fight against tax crime.

Mr. Hassan Zareer

Commissioner General of Taxation

Maldives Inland Revenue Authority

Foreword

This report seeks to encourage and support jurisdictions in the development of domestic manuals for the investigation of tax crimes. Having a comprehensive manual in place to guide law enforcement authorities on the laws and procedures that apply throughout the case lifecycle can enhance the quality, speed, and efficacy of tax crime investigations leading to better enforcement outcomes. The guide provides a detailed outline of the core elements jurisdictions should consider when developing their own domestic manuals and provides a collection of country examples to demonstrate effective investigative practices.

Acknowledgements

This report draws on the domestic tax crime investigation manual prepared by the Maldives Inland Revenue Authority (MIRA), in the context of a joint OECD/UNDP Tax Inspectors Without Borders – Criminal Investigation capacity building programme, where it received support from the Australian Taxation Office (ATO).

This report was written by Emma Scott, Keelan Smith-Connor and Juan Pablo Vargas Serrano of the OECD Secretariat, under the supervision of Marcos Roca. The authors would like to thank the ATO, the MIRA and all the jurisdictions and observer organisations involved in the OECD Task Force on Tax Crimes and Other Financial Crimes for their input and the many country examples that were provided to enrich this report; as well as Laura Gobbi and Sonia Nicolas of the OECD Secretariat for their assistance in finalising the report, and the CTPA Communications team.

Table of contents

Preface 3

Foreword 4

Acknowledgements 5

Abbreviations and acronyms 10

Executive Summary 11

Design, scope, and objectives 13
- Design Considerations 13
- Role of the manual in operationalising the jurisdiction's broader national tax crime strategy 14
- Objectives and scope of the tax crime investigation manual 15
- Periodic monitoring and updates 17

1 Objective of the tax administration and tax crime investigation function 18
- Roles and responsibilities of internal stakeholders 20
- Roles and responsibilities of external stakeholders 22

2 Internal integrity 24

3 Legal framework 28
- Criminal tax offences 28
- Criminal procedures 29
- Evidence collection and management 29
- Taxpayer confidentiality 29

4 Case referral, selection, and allocation 30
- Case referral 30
- Case review and selection 31
- Case allocation 31

5 Case planning 32
- Case direction 32
- Mapping and prioritisation of actions 33
- Resource identification and co-ordination 33

Regular review and recalibration of investigation plan 34
Components of the case plan 34

6 Notifying the suspect they are under investigation 36

7 Powers to identify assets, gather information, and obtain evidence 37

8 Power to obtain documents from third parties 40
Routine third-party notices 40
Non-routine third-party notices 42

9 Covert information gathering processes 43

10 Open source intelligence 45

11 Operationalising a whole of government approach: Domestic inter-agency reporting and information sharing: 46

12 Enhanced forms of inter-agency co-operation 51
Joint intelligence centres 51
Joint investigation or operations 52
Parallel civil and criminal investigations 55
Secondments and co-location of staff 57

13 Government databases and registers available to tax investigators 58

14 The role of whistleblowers in tax crime investigations 60

15 Power to search property and seize physical and digital evidence 62
Physical versus digital evidence 62
Pre-search considerations 64
Obtaining approvals and warrants 64
Formulating a search plan 65
Pre-search orientation meeting 66
Site identification and surveillance measures 66
Command centre 67
Executing the search 67

16 Evidence management 69
Physical evidence 69
Digital evidence 70

17 Asset recovery 71
Asset freezing and seizing 72
Asset management 74
Asset confiscation 74
Enforcement of confiscation orders 78

18 Interview and inquiry 80
Difference between an interview and an inquiry 80
Suspected criminal activity uncovered during an inquiry 81
Responsible authority 81
Initial contact 81
Preparation and delivery of a summon order 81
Planning an Interview 82
Legal warning 82
Right to counsel 83
Interpretation and translation services 83
Interview process 84
Investigation statement and transcript 84

19 Arrest 85

20 International co-operation 86
Informal cross-border co-operation 86
Formal cross-border co-operation 87

21 Investigation case file 92

22 Financial analysis: Direct and indirect methods of proof 94
Useful definitions 94
Net worth/asset betterment method 95
Expenditure method (source and application of funds) 96
Bank deposits method 97

23 Communication standards 99

24 Protecting suspects' rights 100

25 Preparing an investigation report 102

26 Referral for prosecution 103
Role of the prosecution authority at the investigative stage 103
Referral for prosecution 103
Decision to charge 104
Pre-trial proceedings 104
Trial/Hearing 104
Sentencing 105

27 Post investigation procedures 107

References 108

FIGURES

Figure 1. Potential consequences of tax crime 15

Figure 2. Typical life cycle of a tax crime investigation 15
Figure 3. General organisational models for investigating tax crime 20
Figure 4. Key actors involved in a whole of a government tax crime investigation 23
Figure 5. Setting the scene: Defining the case parameters 32
Figure 6. Models for domestic information sharing between agencies responsible for combatting tax crime and other financial crimes 47
Figure 7. Inter-agency reporting in Italy 49
Figure 8. Processes for asset recovery and asset management 71
Figure 9. Types of asset confiscation 77
Figure 10. The power of EOI agreements in combatting tax crime 89

TABLES

Table 1. Core elements of a case plan 34
Table 2. Example process template for issuing a notice to produce information and documents 39
Table 3. Common elements to include in a search plan 65
Table 4. Common elements of search execution 68
Table 5. Management of a digital forensic case 70
Table 6. Key differences between conviction and non-conviction based asset recovery regimes 75
Table 7. Basic differences between interview and inquiry into a person's tax affairs 80
Table 8. Contents of investigation case file 92
Table 9. Useful definitions of evidence and proof 94
Table 10. Formula for net worth/asset betterment method of proof 96
Table 11. Formula for expenditure method of proof 96
Table 12. Formula for bank deposits method of proof 97
Table 13. Fundamental rights of suspects 100
Table 14. Contents of an investigation report 102

Abbreviations and acronyms

AML	Anti-Money Laundering
ATM	Automated Teller Machine
ATO	Australian Taxation Office
CCTV	Closed-Circuit Television
CFT	Countering the Financing of Terrorism
CMS	Case Management System
DTA	Double Tax Agreement
EOI	Exchange of Information
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GST	Goods and Services Tax
HMRC	His Majesty's Revenue and Customs
IFF	Illicit Financial Flows
KYC	Know Your Customer
MAAC	Convention on Mutual Administrative Assistance in Tax Matters
MIRA	Maldives Internal Revenue Agency
MLA	Mutual Legal Assistance
MOU	Memorandum of Understanding
OECD	Organisation for Co-operation and Development
TCIM	Tax Crime Investigation Manual
TFTC	Task Force on Tax Crimes and Other Financial Crimes
TIEA	Tax Information Exchange Agreement
VASP	Virtual Asset Service Provider
VAT	Value-Added Tax

Executive Summary

Tax evasion and other financial crimes have a detrimental impact on all countries. They hinder governments from generating revenue and erode public confidence in government and the financial system. This can result in wide-ranging negative outcomes as resources are diverted away from critical public services and infrastructure, and in many cases, used to finance other serious crimes, such as money laundering, corruption, the trafficking of goods and people, and terrorist financing.

In 2022, the Council of the Organisation for Economic Co-operation and Development (OECD) adopted the Recommendation on the Ten Global Principles for Fighting Tax Crime (OECD, 2022[1]); the first global reference guide setting out the ten essential principles jurisdictions should have in place to efficiently and effectively prevent, detect, investigate, prosecute and recover the proceeds of tax crimes.

Effective implementation of these principles at the domestic level requires, among other things, operational guidance that tax and other law enforcement authorities can rely on to guide their investigations of tax crimes. However, through the work of the OECD Task Force on Tax Crimes and Other Financial Crimes (TFTC - https://www.oecd.org/en/topics/sub-issues/standard-setting-for-tax-and-crime.html) and related capacity building programmes, it has emerged that some jurisdictions may lack comprehensive practical guidance for operational officials relating to the investigation of tax crimes. This lack of guidance is compounded by the fact that in many jurisdictions, responsibility for tax crime investigations is often divided between the tax administration and other law enforcement authorities, resulting in potential misalignments between possessing the technical knowledge and having the adequate legal powers for investigating complex tax crime cases

Against this background, OECD Members agreed that the TFTC would develop a guidance tool to encourage and support governments with the development of their own domestic manuals for the enforcement of tax crimes.

The development a comprehensive tax crime investigation manual (“TCIM” or “manual” hereafter) can be beneficial in enhancing the efficacy and efficiency of tax crime investigations. It can:

- serve as a guiding framework to help streamline the investigative process. This can enhance both the quality and speed of investigations;
- provide clear protocols and procedures that contribute to the timely resolution of investigations by minimising the potential for delays caused by uncertainty or indecision;
- offer criminal investigators quick and easy access to the legal and operational frameworks and procedures that govern their enforcement powers, ensuring strict compliance with criminal procedures, in particular safeguarding evidence for admission in court and respecting applicable procedural rights of the suspect.
- clearly define, in one place, the institutional arrangements for the agency or agencies involved in fighting tax crime, supporting the appropriate allocation of human, financial, and technology resources;

- provide guidance on the use of technological resources, augmenting officers' investigative capabilities; and
- support the integration of global best practices into each jurisdiction's domestic processes, thus strengthening both domestic, regional, and global efforts to fight tax crimes and related illicit financial flows.

In effect, a well-developed TCIM can serve as a key tool for efficient and effective investigative processes. To that end, the suggested topics for inclusion in a manual are wide-ranging, spanning detailed guidance on the various stages of a tax crime investigation life cycle, including case referral, selection and allocation; case planning, information and evidence gathering; analysis of information; the decision to charge; referral to prosecution; sentencing; and recovery of assets. The manual also covers more practical aspects such as the roles and responsibilities of different agencies, teams, and individual; standards for internal and external communications; and the importance of upholding suspects' rights. Every aspect of the manual should ideally include references to the underlying legal framework.

To make the tool as simple to use as possible, it has been developed to serve as an outline or template that jurisdictions can adapt when developing and/or updating their own domestic guidance and manuals on criminal tax investigations. To that end, the chapter headings and section titles throughout the document can be treated as indicators of topics that any domestic TCIM could cover.

Caveat

Tax crime enforcement agencies operate in varied environments, and the way in which they each administer their work and interface with other financial crime agencies differs in respect to their policy context, legislative environment, and administrative practice and culture. Whilst the core aim of a TCIM should be to guide tax investigators through the life cycle of an investigation, due regard needs to be paid to the distinct circumstances, challenges and priorities each agency and jurisdiction is managing, and a standard approach to criminal tax investigations may be neither practical nor desirable. This document is therefore intended to assist administrations in their domestic considerations regarding the development and implementation of an efficient and effective TCIM.

Design, scope, and objectives

Design Considerations

When considering the development of a TCIM and/or updates to existing guidance, governments should consider the format(s) in which it will be made available. The design of the manual will be dependent on several factors unique to the jurisdiction, including the domestic legal framework as well as specific risks, requirements, preferences, resourcing, and technological capabilities of the agency mandated to fight tax crime.

While it is critical that the TCIM is fit for purpose for its end users, the investigators, in light of the rapidly evolving technological landscape in which tax authorities and law enforcement operate, it is strongly encouraged that all jurisdictions make their manual available in a digital format. This will make it easier to link related topics and materials both within the manual and externally, providing a more enriching and accessible learning tool, including one that can be consulted in the field. Digital formats also offer more flexibility for updating content, allowing the manual to become a living or evergreen document, ensuring that the end-user always has access to the most current information. Moreover, digital manuals contribute to a more sustainable environment by reducing production, dissemination, and distribution costs and associated environmental prints and impacts.

Key considerations when designing the TCIM include:

- **Format:** Will the TCIM be available digitally, physically, or both?
- **Categorisation:** Will the TCIM be organised chronologically in order of the investigation life cycle, alphabetically or in some other way?
- **Where will the TCIM be used,** for example for desk-based investigations or in the field. In some instances, more than one format may be appropriate (e.g. a pocket-field TCIM for conducting searches of property in remote locations with no internet access or ability to charge devices);
- **Access to technology:** Does the jurisdiction have the digital resources and infrastructure to support the use of a digital TCIM?
- **Interfacing:** For example, linking relevant procedures to their related templates/forms to promote the standardisation of processes and consistency in their execution.
- **Searchability:** For example, the ability to search by topic or keywords and to link related topics;
- **Accessibility:** For example, where will the TCIM be housed and what are the limits of accessibility of particular locations, and what are the security implications.

Box 1. Examples of publicly available tax crime investigation manuals in the United States and Kenya

The United States' Internal Revenue Service (IRS) makes all its staff manuals (https://www.irs.gov/irm) publicly available on its website. This includes Part 9, which outlines the criminal investigation process in detail. (Internal Revenue Service, 2023[2]). Likewise, the Investigation and Enforcement Department of the Kenya Revenue Authority (KRA) publishes a taxpayer edition of its Tax Investigations Handbook https://www.kra.go.ke/images/publications/KRA-TAX-INVESTIGATION-FRAMEWORK-1.pdf) on its website. (Kenya Revenue Authorithy, 2019[3])

Role of the manual in operationalising the jurisdiction's broader national tax crime strategy

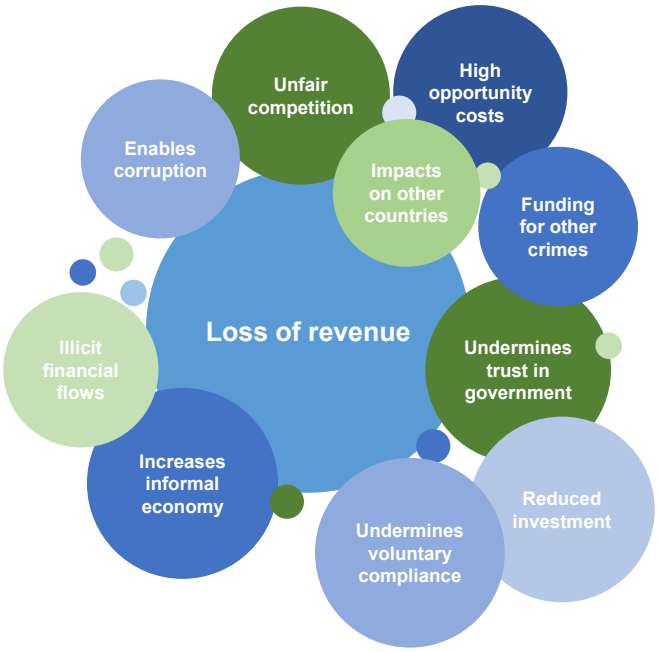
Principle 2 of the OECD Recommendation of the Council on the Ten Global Principles for Fighting Tax Crime (hereafter, "the TGP Recommendation") (OECD, 2022[1]) recommends that jurisdictions:

> *Devise a strategy for addressing tax crimes, which includes: a) the identification of existing and emerging risks and threats; and b) mechanisms for the regular review and monitoring of the implementation and effectiveness of the strategy.*

The OECD elaborated on how to develop such a strategy in its publication Designing a National Strategy against Tax Crime: Core Elements and Considerations (OECD, 2024[4]). In essence, it is advised that jurisdictions should have a national, whole-of-government strategy for countering tax crime which focuses on the jurisdiction's main risks (both existing and emerging); sets clear objectives and priorities; and is subject to periodic monitoring. An effective strategy will help counter the wide-ranging negative consequences of criminal tax behaviour. (See: Figure 1)

Mechanisms should be in place to ensure the actual implementation of the strategy, including by conducting coherent case selection and efficient investigations. In this regard, the TCIM should serve as a guide for investigators on how to efficiently investigate suspected offences in a transparent, fair, and systemic manner.

Figure 1. Potential consequences of tax crime



Source: (OECD, 2024[4])

Objectives and scope of the tax crime investigation manual

A suitable starting point for all jurisdictions considering developing their own TCIM is to first consider the purpose for which it is being developed and the outcomes they hope to achieve with the resource.

An effective TCIM should offer comprehensive guidance encompassing both general principles for conducting investigations and detailed commentary, along with templates and checklists addressing specific aspects within an investigation. While the lifecycle of an investigation will vary between countries, in general the TCIM should cover the role of the investigator at each critical stage of an investigation.

Figure 2. Typical life cycle of a tax crime investigation

Source: OECD, 2025

At a minimum, the TCIM should be designed to:

- **Act as a primary reference point for criminal tax investigators** on the procedures and processes to follow at all stages of an investigation. These processes can be complemented with detailed commentary, worked examples, real-world cases, document templates and checklists to support investigators navigating what can often be complex situations.

- **Standardise and institutionalise staff processes:** A manual can create a primary repository of operational procedures for staff to follow. Simple, clear, and easy to follow written instructions reduce the risks of errors occurring and promote uniform and consistent outcomes.
- **Enhance compliance:** Paramount to all processes within any tax crime investigation agency should be ensuring that investigators exercise their mandated powers in a compliant and impartial manner, respect the rights of suspects, and ensuring that whistleblowers and other informants are appropriately protected.
- **Increase transparency:** Making a manual available publicly can provide transparency to taxpayers, their representatives, and the general public regarding how certain decisions are made as well as requirements necessary for officers to follow. This, in turn, increases staff adherence to the processes, creates accountability, and mitigates the risk of complaints from external stakeholders. However, jurisdictions may wish to keep certain aspects of a TCIM confidential if, for example, it might allow criminals to thwart investigations.
- **Raise awareness of and promote the effective use of available powers:** A manual can provide a centralised index of the full range of tools and powers available to criminal investigators, and relevant tax crime investigations agencies, supporting officers' decisions and the use of the most appropriate powers.
- **Optimise the use of agency knowledge and resources:** Processes within a TCIM can be complemented over time through the inclusion of best practices and success stories observed by investigators in their roles so they can be shared and adopted across the entire agency. Furthermore, a manual can also be used as a directory to create awareness about any specialist teams to which processes can/should be outsourced, such as forensic accountants, data analysts, or other subject matter experts.
- **Operationalise a whole of government approach to combatting tax crime:** Combatting tax crimes effectively requires co-operation between various government agencies. To that end the TCIM should clearly establish the role of all agencies mandated to fight tax and other financial crimes and the laws and mechanisms in place for them to report and share information with each other and collaborate more broadly.
- **Support the effective onboarding of new staff:** A well drafted TCIM can expedite the orientation of new investigators by providing them with a one-stop reference guide containing necessary and relevant information to conduct their own criminal investigations as they go.
- **Ongoing learning and development:** A manual provides a reference tool to educate and guide staff on the application of new policy or legislative changes (including court decisions) to ensure that all staff are aware of when and how these must be operationalised.

It is necessary to acknowledge that no manual can provide a solution to every situation an investigator may encounter during an investigation. The manual should, as necessary, refer to statutes and laws and other material that should be consulted in certain situations, and provide advice about where engagement with senior managers and/or legal advisors might be necessary. It should also be clear on where investigators have a degree of flexibility to apply their own critical thinking, training and professional experiences to their investigations. In this way, the manual should guide the investigative process, fostering the potential for innovative and alternative approaches that could themselves enhance an approach or process already within the manual.

Periodic monitoring and updates

For a TCIM to be effective, it is critical that it is reviewed and updated on a periodic basis. For example, updates may be made, to reflect successful practices, to take into account mistakes made in past investigations, and/or to keep pace with changes to legislation, regulation, or developments in case law.

To that end, it is strongly recommended that the manual itself outline upfront the internal governance process for monitoring and review, including the frequency with which it should be reviewed and the teams assigned conduct the review. An example of how this is managed in the United Kingdom is included in the box below.

Box 2. Management of procedural updates to staff handbook in the United Kingdom

His Majesty's Revenue and Customs (HMRC) in the United Kingdom maintains a Fraud Investigation Service (FIS) Handbook; an electronic platform which acts as the primary reference point and source of guidance for all FIS operational investigation staff, particularly when dealing with complex or unusual cases. It encompasses over 200 subjects, including guidance, policy and mandatory instructions, each overseen by dedicated Subject Owners (subject matter experts). Regular reviews and updates are conducted on an ongoing basis to ensure that the content reflects changes in legislation, case law, best practice and technical developments.

Source: HMRC, United Kingdom (2025)

1 Objective of the tax administration and tax crime investigation function

A TCIM should begin with an introductory section which sets out, among other things,

- The objectives of the tax administration and/or the crime investigation agency;
- The role of the manual in operationalising the jurisdiction's national tax crime strategy;
- The purpose of the TCIM, as well as the limitations on its use (for example the need to refer to other materials).

Modern tax administration systems are largely based on self-assessment and voluntary compliance. The role of criminal tax investigation is to detect and investigate suspected breaches of the law and to thwart attempts to abuse the tax system by engaging in criminal offences. Successful prosecutions, the imposition of sanctions and effective recovery of criminal proceeds will also serve to disrupt and deter criminal offending.

All employees within a tax administration should have a general understanding of their organisation's overall strategic objectives as well as the role that tax crime investigation plays in the achievement of the agency's objectives. Outlining to criminal investigators both the broader mandate of their agency as well as defining the purpose of their role provides a foundational basis that can help guide and inform investigators in their decision making as well as help facilitate closer and more joined-up investigations. Furthermore, it is also advisable to outline the role of the agency as part of the jurisdiction's whole-of-government approach to combatting tax crimes and other illicit financial flows.

To that end, the manual should include a clear description/mission statement of the tax administration and the role of criminal tax investigations (whether housed within or outside of the tax administration). Examples of mission statements from the Maldives' and Norway are set out below.

Box 3. Mission Statements from the Maldives and Norway

Maldives Inland Revenue Service

Fostering public trust in the tax system is bolstered by a tax administration system that is fair, transparent, and equitable. Maldives Inland Revenue Agency's (MIRA) Strategic Plan underscores the importance of implementing credible enforcement measures against those abusing the tax system to sanction the offenders and to create a deterrent effect on other noncompliers.

Tax Investigation is one of the actions taken by MIRA to tackle taxpayers with severe non-compliance. The purpose of a tax investigation is to uncover the truth by investigating the alleged criminal (tax) behaviour. In conducting a tax investigation, MIRA officers will generally seek to find and analyse information for the purposes of determining whether or not a tax crime has been committed.

Source: Maldives Inland Revenue Authority (2025).

National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)

"Norway is a good country to live in – we have many values to protect"

Norway is a democratic state governed by the rule of law with fairly harmonious political conditions and basic agreement on the rules of the game for conflict resolution. Norway is a welfare society with a relatively high degree of social and economic security. Norway has a regulated market economy with well-developed legal rules for trade, competition and working conditions in the business sector. Norway has a beautiful nature with rich resources both on land and at sea as an important basis for economic activity and recreation. In short, we have a number of important values to protect.

Crime is a threat to these values. Tax and duty crime undermines the public sector's revenue base and threatens the welfare state. Like fraud with public subsidies and support schemes, such crime has a distorting effect on competition and creates mistrust between businesses and between the public sector and citizens. Other violations of the rules of the road in the business sector, for example in connection with bankruptcy crimes and violations of competition rules, also undermine the relationship of trust with both customers and the rest of the world. Securities crime destroys confidence in the securities market and weakens access to capital for the business sector. Corruption in the business sector or in public bodies creates mistrust and can force a control society that we do not really want. Money laundering makes it difficult to detect all forms of economic crime and, in the worst case, undermines the government's economic policy. Certain forms of environmental crime threaten the natural environment. And so on.

Through their work to combat economic crime and environmental crime, the employees of Økokrim contribute to protecting important values in Norwegian society.

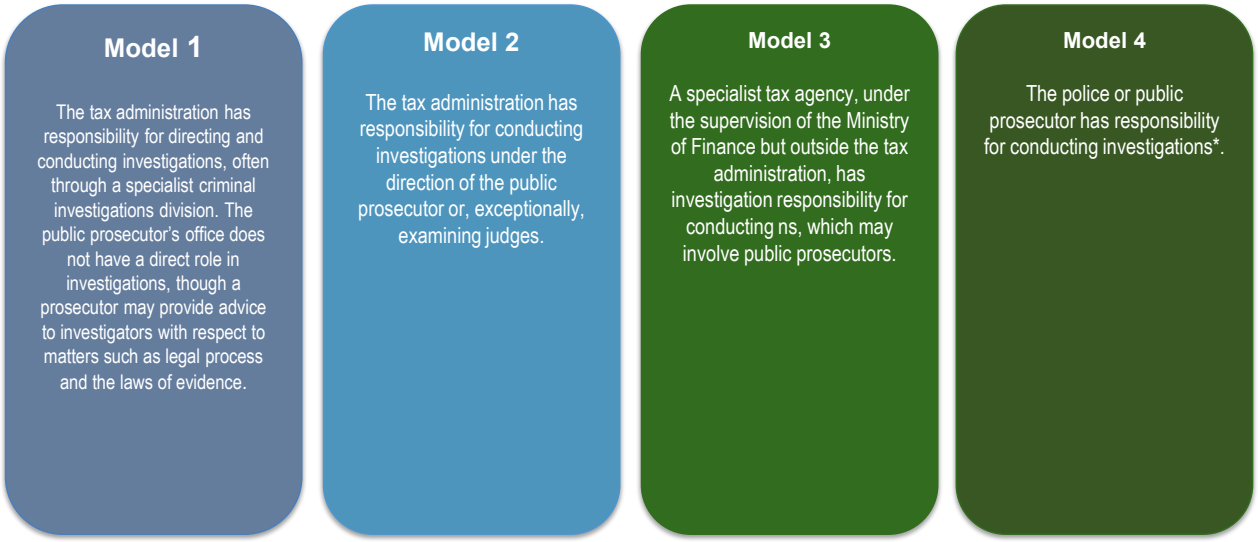
Source: www.okokrim.no/historie-og-samfunnsoppdrag.562405.no.html

Principle 5 of the TGP Recommendation recommends that jurisdictions put in place an organisational structure with defined responsibilities for fighting tax crimes and other financial crimes (OECD, 2022[1]). To support this, the TCIM should clearly define the roles and responsibilities of key internal and external stakeholders in criminal tax investigations. Ensuring that each individual, team, unit, and agency is aware of their respective role in criminal tax investigations will help avoid duplication of efforts, prevent any oversights, and ensure appropriate allocation of resources.

Roles and responsibilities of internal stakeholders

To ensure effective and efficient case management, the TCIM should clearly define the roles and responsibilities of different members of the investigation team as well as the wider internal structures that support the criminal investigation function (e.g. audit, intelligence, information exchange, international co-operation, legal etc.). This structure will necessarily differ depending on the legal and operational context of each jurisdiction, and by whether the tax crime investigation function resides within or outside of the tax administration. The figure below shows four general organisational models that countries adopt for investigating tax crimes.

Figure 3. General organisational models for investigating tax crime



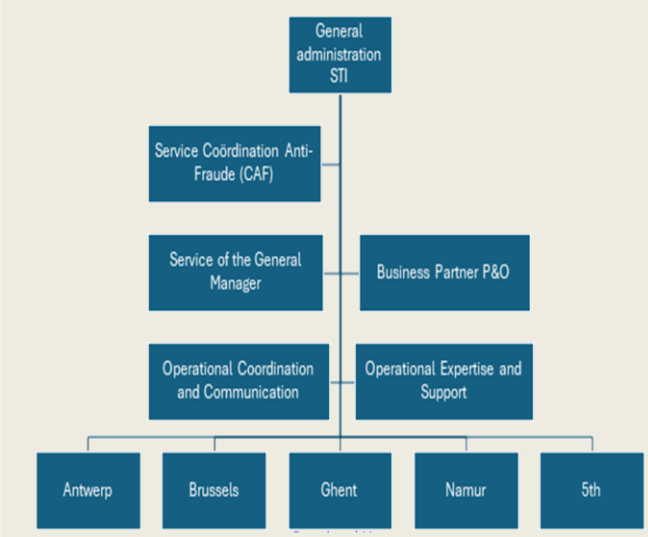
*The investigative team may be supported by tax auditors/investigators if the law authorises it.
Source: (OECD, 2017[5])

Regardless of the structure, the TCIM should create an awareness of all units that support the investigation function. This could be done by way of the inclusion of an organigram with corresponding descriptions of the roles/responsibilities of the relevant individuals, teams, and units. An example of the internal structures in Belgium and Kenya are included in the box below.

Box 4. Organisational frameworks for fighting tax crime in Belgium and Kenya

Fighting serious and organised tax evasion in Belgium

The Belgian Special Tax Inspectorate's (STI) mission is to fight against serious and organised tax evasion. For this reason, STI is authorised to check the tax situation of any person liable to tax as regards any tax and duty, whose assessment, control, or recovery are ensured by the State. In accordance with its "key mission" STI is mainly in charge of examining fraud cases connected to organised economic and financial crime, in particular:



- Offences in connection with serious and organised tax evasion, which uses complicated mechanisms or international processes (e.g., when it concerns "carousel fraud schemes")
- Financial swindling;
- Fraudulent use of corporate property;
- Fraudulent organisation of insolvency.

STI mainly carries out missions as regards control and taxation but also intervenes at all levels of the litigation procedure. In this respect it enjoys the support of legal offices, which also play an important role with regards to technical and legal assistance to taxation services.

On top of that, STI has at its disposal a mobile recovery office which "ensures" the later recovery of STI's taxations. In close collaboration with the competent collectors of the Administration of Tax Recovery, it takes the necessary initiatives to ensure the effective recovery and to stop the fraudulent organisation of insolvency.

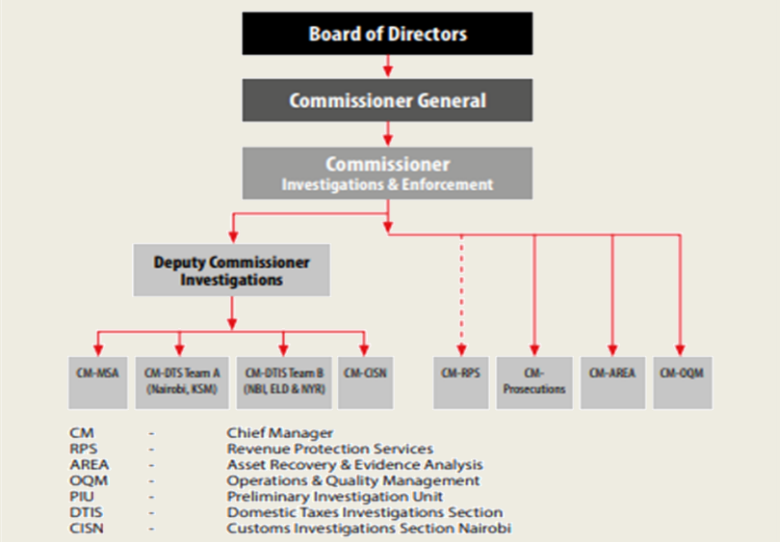
STI has five (regional) directions: Antwerp, Brussels, Ghent, Namur, and the 5th Direction (which covers the entire country). The International Co-operation Service which makes up part of the division of "Operational Expertise and Support" provides assistance to investigation teams in the context of their tax audits when it is necessary to obtain information held abroad. It is responsible for keeping abreast of international tax issues, in particular all aspects relating to the exchange of tax information in all its forms, and participates in international workshops (Fiscalis, OECD, IOTA, Benelux Union, etc.). It also maintains contacts with foreign tax administrations and international organisations such as the OECD, Eurofisc, IOTA, etc.

The mission of the Service Co-ordination Anti-Fraud (CAF) is to co-ordinate the co-operation between services that are directly or indirectly responsible for combating various forms of fraud. This includes, on one hand, co-operation with various external services such as the Public Prosecutor's Office, the Federal Public Service (FPS) Economy, Foreign Affairs, Justice, the CFI, and the Federal Police. On the other hand, the CAF is responsible for co-ordination within the FPS Finance as a single point of contact (SPOC): "UNA VIA", amicable settlements, tax havens, and anti-money laundering.

Source: FPS Finance, Belgium (2025).

Combatting tax crimes in Kenya

The Kenya Revenue Authority (KRA) is the central agency responsible for the assessment, collection, and enforcement of tax laws and other central government revenue laws in Kenya. The Investigations & Enforcement Department (IED) is comprised of seven units tasked with detecting, disrupting, and deterring violations of tax law.

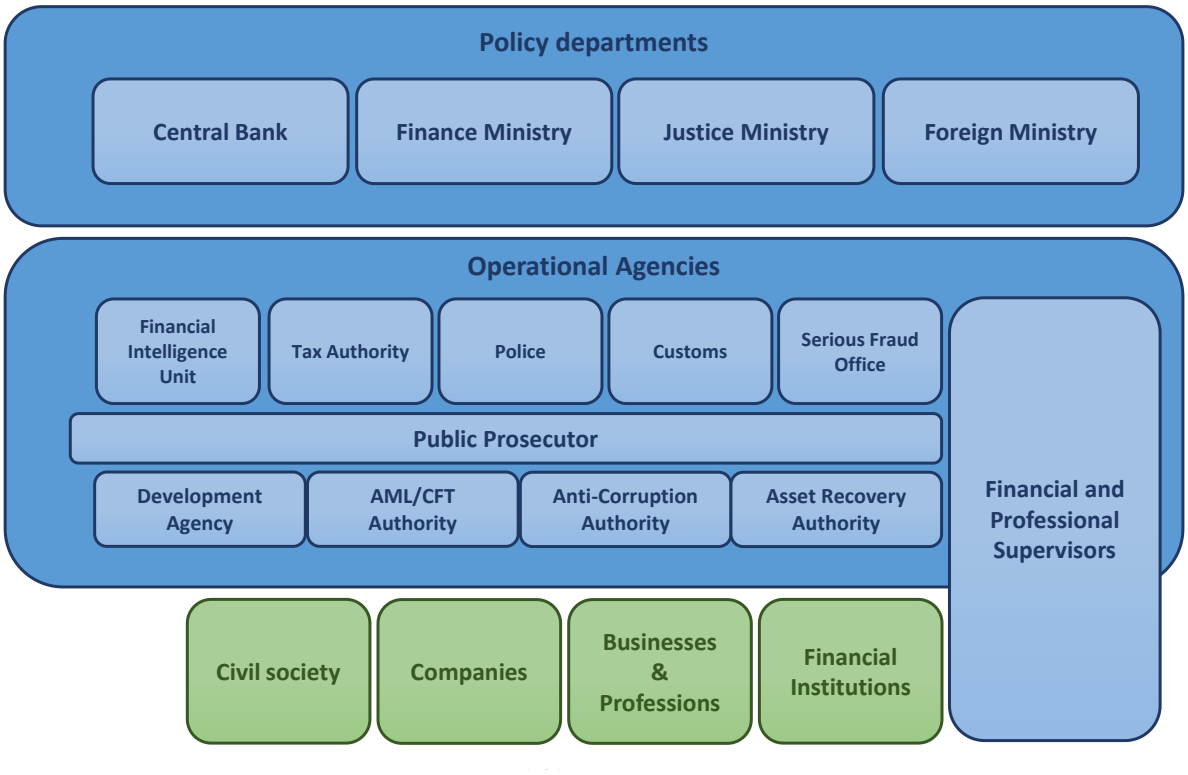


Source: Kenya Revenue Authority (2019). Tax Investigations Handbook. Taxpayer Edition. Investigations and Enforcement Department, www.kra.go.ke/images/publications/KRA-TAX-INVESTIGATION-FRAMEWORK-1.pdf

Roles and responsibilities of external stakeholders

Tax crimes are inherently linked to a range of other criminal conduct such as bribery and corruption and terrorist financing and are therefore a common predicate offence for the crime of money laundering. Combatting these crimes and the illicit financial flows (IFFs) they generate requires jurisdictions to adopt a "whole-of-government" approach to detection and enforcement. This approach emphasises collaboration and co-operation across the various operational agencies, policy departments and ministries involved in fighting IFFs, each of whom hold a range of information that can be critical to the enforcement of crimes within each other's respective mandates. Sections 13-15 outline in more detail the various forms of reporting, information sharing, and other types of collaboration that can take place between different financial crime agencies. However, the first step should always be to identify who the key stakeholders are. While the list of key stakeholders, their role, and the level of co-operation between them will vary between jurisdictions, the figure below identifies key stakeholders that are common to many jurisdictions.

Figure 4. Key actors involved in a whole of a government tax crime investigation



Source: (OECD, 2024[4])
Note: The top level is the key policymaking departments in central government. IFFs do not sit within the normal remit of a single ministry but cut across several departments. The middle level includes the operational agencies which implement the laws, regulations, and policies to counter IFFs – both preventive and punitive. This includes part of the criminal justice system; financial and professional supervisors; and a range of specialised agencies. The lower level shows the sectors outside government which have a role in applying measures to prevent and detect IFFs, of which there are many. For example, 'businesses and professions' in this case applies to accountants, auditors, lawyers, notaries, dealers in gemstones and antiquities, real estate agents, company formation agents, financial advisors, and several others.

In addition to identifying key external stakeholders, the TCIM should provide information on when and how they should be consulted at particular stages of an investigation. While this will be outlined in more detail throughout the relevant sections of the TCIM, it is useful to include upfront a section with the various agencies' mandates, to ensure that investigators are aware of the different actors that can and should be involved/consulted at critical stages of an investigation for example, for surveillance, service of document, search and seizure, summons, digital forensic analysis, obtaining evidence mutual legal assistance, etc.

2 Internal integrity

Tax and financial crime investigators, must be held to the highest degree of ethical and integrity standards. Any form of misconduct within an investigation authority can jeopardise the investigation and its results. Internal integrity units within tax administrations and law enforcement authorities play a critical role in upholding public trust and accountability within an organisation and maintaining ethical standards. Some key functions of internal integrity units are outlined below.

Investigation of misconduct: Typically, the principal function of an internal integrity unit is to investigate any allegations of misconduct (whether internal or external) by authorities working within the tax administration and/or law enforcement authority. This could be an administrative investigation into employment related misconduct (e.g. harassment) or a criminal investigation into suspected illegal activity (e.g. corruption, embezzlement, breaches of taxpayer confidentiality, conflicts of interest, etc.). As part of this role, the unit is often responsible receiving internal reports of misconduct and for the establishment and management of dedicated reporting channels for both internal and external whistle-blowers.

Prevention of misconduct: Internal integrity units play a crucial role in maintaining the accountability of criminal tax investigators through the implementation of measures such as background checks on prospective employees, declarations of interests and assets, identification and oversight of units or individuals susceptible to unethical conduct, and lifestyle audits for unexplained wealth. In this sense, the mere presence of the unit can serve to hold investigators to account.

Promoting a culture of integrity: Integrity units are often responsible for the development and oversight of internal codes of conduct, anti-corruption policies, and the delivery of associated staff training on ethical standards.

Accountability: The unit often has a role in supporting the internal audit function of the organisation, managing internal affairs such as cases involving law enforcement officers, and reviewing cases that may warrant increased oversight and/or further investigation.

Enhancing transparency: Integrity units play an important role in fostering public trust in the organisation by communicating with the public directly on high profile cases, particularly in instances where a decision is made to close an investigation of a public official without any charges.

More broadly, internal integrity units within tax administrations and law enforcement authorities can play an important role in protecting the integrity of the wider public sector through the detection and reporting of suspected criminal activity by public officials.

The TCIM should educate and raise awareness among investigators of the role of their organisation's internal integrity unit, including:

- A description of key roles/functions of the unit;
- Links to all relevant internal codes of conduct, anti-corruption policies, etc;
- Information regarding any compulsory staff training on integrity matters;
- Information on investigators' obligations for reporting suspected misconduct within the organisation and associated reporting channels;
- Its role with respect to internal and external whistleblower reporting.

Box 5. Promoting internal integrity in Italy and in the United Kingdom

Prevention of unethical behaviour by Italy's Guardia di Finanza

Italy's Guardia di Finanza prevents any unethical behaviour of its personnel by annually drawing and updating its own three-year plan for the prevention of corruption and transparency.

This document maps out the working processes at risk of corruption performed by the Corps' members, identifies the main corruption risks, the relevant prevention measures and the monitoring methods. Furthermore, it establishes measures for the prevention of corruption risks, which can be:

- **General:** aimed at preventing risks relating to all work processes, example, staff rotation, the promotion of transparency, the obligation to abstain in the event of conflicts of interest, the procedures to be followed for the conferral and authorisation of extra-institutional assignments, the methods for verifying the legitimacy of activities following termination of service;
- **Specific:** related to individual working processes, such as those adopted in public competitions.

To this end, since 1996, the Guardia di Finanza has set out the rules of conduct to be observed by its personnel, adopting its own Code of Conduct and each year provides training on the issues covered therein to approximately 17,000 staff members. It also activated its own internal reporting channel under Legislative Decree no. 24/2023, the so-called "whistleblowing".

The Guardia di Finanza institutional website, since 2013, also features a 'Transparent Administration' area, aimed at hosting the data and documents subject to mandatory or optional publication. Furthermore, every year, the Corps provides about 5,000 members with training on the management of ethical issues, procedures for submitting "whistleblowing" reports, corruption prevention systems, risk management, transparency and access to public information.

Supervisory and control functions are a fundamental aspect of the command action at all levels and characterise an organisation branched out with around 60,000 members over the whole Country and hierarchically structured.

Internal controls are carried out in many and various ways and concern all work processes.

All the activities carried out by the *Guardia di Finanza* members, in any institutional field and sector, are subject to specific directives and targeted reporting (also with special IT systems) that guarantee the traceability and objectivity of the information contained therein and allow easy verification of the correctness, adequacy, and consistency of the data entered by each staff member with respect to the tasks and duties assigned to the same. As an example, every single access to the many operational databases available to the Corps must be justified on a special register kept in each Unit, is subject to log procedures and is monitored by higher supervisors. The involvement of several supervisory levels in the control system guarantees autonomy of assessment and a greater possibility of detecting any conduct contrary to the integrity of the Administration.

Source: Guardia di Finanza, Italy (2025).

Upholding internal integrity within the United Kingdom's His Majesty's Revenue & Customs

HMRC maintains a mature internal integrity unit. Internal Investigations is a wholly independent investigative body based within the HMRC Fraud Investigation Service. Its core purpose is to protect HMRC's integrity and reputation and help to maintain public trust and confidence.

HMRC has adopted UK National Protective Security Authority terminology when considering internal integrity and has developed and adopted an effective Insider Risk governance structure in tackling internal attacks against HMRC's infrastructure and reputation. Internal Investigations is very much focussed on surfacing and responding to Insider Events. Wider business stakeholders have responsibility for managing Insider Risk and mitigation of Insider Threats.

Internal Investigations has a whole business remit addressing and investigating misconduct, internal fraud, and corruption wherever it may surface in HMRC. It maintains accredited teams delivering intelligence development, civil misconduct investigations, and criminal anti-corruption investigations considering and applying the most appropriate response to insider threats presented by staff.

Operationally Internal Investigations benefits from its association with the Fraud Investigation Service, maintaining legal powers of arrest and search, and being able to call on additional criminal investigation capacity where operational needs require, and operational security restrictions allow. Effective and important links are also maintained with wider UK law enforcement agencies, particularly police Professional Standards and Anti-Corruption units.

Internal Investigations invests resources in surfacing organisational learning from its operational activities, working with stakeholder partners such as HMRC's personnel security functions and Human Resources to ensure lessons are learned and prevention messaging is shared more broadly across HMRC employees to promote good conduct and deter corruption.

Source: HMRC, United Kingdom (2025).

Box 6. Examples of criminal conduct uncovered by internal integrity units in Hungary and the United Kingdom

Internal investigation leads to dismantling of extensive VAT fraud network in Hungary.

In 2017, the Public Prosecutor's Office of Hungary, acting as investigating authority, contacted the internal integrity unit of the National Tax and Customs Administration (NTCA) and asked to determine whether a certain NTCA employee had lawfully conducted data queries on 2-3 specifically named companies.

The internal investigation found that the employee had unlawfully queried more than 25 companies. Furthermore, it was identified that all the entities queried by the former colleague had been established in the previous 2-3 weeks and were starting to reclaim VAT. Ultimately, the internal investigation revealed that the NTCA employee was continuously monitoring the VAT claims and where the internal systems had flagged the company's VAT lodgement for audit, those companies had coincidentally been deregistered very soon after.

The investigating authority, supported by the data and information uncovered by the internal integrity team, were able to identify that other persons co-operating with the NTCA employee had approached homeless people and other individuals who did not have a tax identification number. Their investigation revealed that the employee undertook steps to regularise the tax affairs of these people and again monitored their cases as they were processed. Once their tax situation was corrected, these persons set up companies and began claiming VAT refunds. It was also established that the same lawyer, in co-operation with the former NTCA employee, had facilitated the lodgments in each case.

As a result of the involvement of the NTCA internal integrity unit in the Public Prosecutor's Office's investigation, an extensive VAT fraud network was dismantled. This case example shows that co-operation between domestic agencies, including their internal integrity units, can provide effective assistance in the detection and disruption of tax and financial crimes.

Source: National Tax and Customs Administration, Hungary (2025).

HMRC officer guilty of misconduct in public office

Whilst employed by the United Kingdom's His Majesty's Revenue & Customs, a senior tax compliance officer, with prominent UK businesses in her compliance portfolio, married a recidivist fraudster who had served prison sentences on several occasions. HMRC conducted a covert operation linking both the Senior Tax Officer and her husband to the laundering of £3.3 million through multiple bank accounts. It was clear that they were living a life beyond their means with access to high value assets and lavish holidays. It was established that the Senior Tax Officer used her system accesses and insider knowledge to generate false HMRC letters with false identities which were then used by her husband to open the bank accounts used to layer the criminal funds. Both individuals were criminally prosecuted, the husband pled guilty to money laundering and the Senior Tax Officer was dismissed following arrest and pled guilty to Misconduct in a Public Office.

Source: HMRC, UK (2025).

3 Legal framework

Every stage of a tax crime investigation relies on an underlying legal framework that not only defines what constitutes a criminal tax offence, but also sets out the obligations and rights of taxpayers and the roles, powers, and responsibilities of those mandated to enforce the law. This is critical for maintaining the rule of law and ensuring that justice is carried out in a fair and consistent manner. It is therefore critical that all tax crime investigators are familiar with the key legislation that governs their functions.

To that end, every legal power, process, procedure, etc. included throughout the TCIM should include a specific reference to the underlying legislation, including where possible, links to where the legislation can be found online (e.g. on a publicly available website, hard copies in an agency library, etc.) as well as the contact details of any subject matter experts or internal legal teams who can provide advice. Moreover, it is useful to include a short chapter upfront that identifies the key pieces of legislation that underpin the jurisdiction's broader frameworks for the enforcement of tax crime.

While this will vary among jurisdictions, the chapter should, at a minimum identify what legislation governs criminal tax offences, criminal procedures, evidence collection and management, and taxpayer confidentiality.

Criminal tax offences

As set out in Principle 1 of the Ten Global Principles, and for the purposes of this guidance document, tax crime refers to conduct that violates a tax law and can be investigated, prosecuted, and sentenced under criminal procedures within the criminal justice system (OECD, 2021[6]). It covers the violation of both income tax law obligations, as well as indirect tax obligations (such as VAT or GST), but it does not include other financial crimes such as the violation of customs and excise taxes, corruption, bribery, or money-laundering laws. However, these crimes will of course also be relevant for criminal tax investigators, who will need to be able to identify and refer suspicions of such crimes to the competent authority and support with their investigations as needed (see section 12 on inter-agency co-operation).

The TCIM should identify all criminal tax offences in the jurisdiction, whether set out in specific tax legislation, a criminal code, or both. The section should also detail whether the offence(s) apply to:

- Individuals and/or legal entities;
- Those who aid, abet, counsel, enable or are otherwise complicit in the offence; and
- Those who attempt or conspire to commit an offence.

Moreover, the description of each offence should include:

- A description of the statute of limitations, including its length, when it commences, reasons for pause or suspension, etc. This is critical for ensuring that time is not wasted pursuing crimes that are outside of their limitation period.
- Available sanctions (e.g. civil and/or administrative fines, criminal fines, imprisonment, etc.).

Criminal procedures

Most jurisdictions will have detailed legislative and regulatory frameworks governing the procedures that must be followed in criminal investigations (e.g. a Criminal Procedure Act or Code). These frameworks are intended to safeguard against arbitrary and unjust treatment of suspects, prevent miscarriages of justice, uphold the rule of law, and ensure the fair and efficient administration of criminal justice, ensuring public confidence in the work of the criminal justice system.

In general, criminal procedure legislation will outline the steps that law enforcement authorities and the courts must follow during an investigation, arrest, charging, pre-trial proceedings, trial, sentencing, and appeals, among others. To that end, criminal procedure laws will underpin much of a jurisdiction's TCIM and should be referenced frequently throughout to ensure that the rules are clear and accessible to all tax crime investigators.

In some jurisdictions, the criminal procedures may differ depending on the seriousness of the offence. For example, investigators may be able to employ a broader range of investigative techniques for more serious offending. To that end, this section should also highlight where there is any deviation in the procedures that apply to different tax crimes.

Evidence collection and management

Legislation that governs evidentiary procedures for criminal matters will also play a central role in the TCIM (e.g. an Evidence Act). This legislation is critical for ensuring that the evidence presented in court is relevant, reliable, and obtained in a manner that respects legal rights and the principles of justice. These laws typically outline the types of evidence that are permissible, such as testimonial, documentary, and digital evidence, and set forth the procedures for presenting and challenging evidence. Evidentiary laws also establish the standards for evaluating the weight and sufficiency of evidence, which are crucial for fair and accurate decision-making by judges and juries. Finally, evidence laws typically include provisions for the protection of sensitive information and the rights of witnesses and parties involved in a case.

The proper application of these laws is critical for effective law enforcement and the protection of civil liberties. Therefore, tax crime investigators must either possess, or have access to a legal department with a thorough understanding of the provisions outlined in law and how they must apply in particular circumstances.

Taxpayer confidentiality

Taxpayer confidentiality is of the utmost importance to the integrity of the tax and justice systems. To that end the manual should clearly identify the legislation that governs taxpayer confidentiality and when and how taxpayer information may be disclosed or shared outside of the tax administration.

4 Case referral, selection, and allocation

A systematic approach to the referral, selection and allocation of criminal tax cases is critical for ensuring consistency and fairness while adhering to legal frameworks.

Case referral

An effective TCIM should detail the various ways that a tax crime case may be referred to the criminal investigation team for investigation. For example,

- **Intelligence Analysis:** Most modern tax administrations have an intelligence function that is responsible for detecting and analysing the risk of tax evasion and fraud. Where such risks are detected, the intelligence team or unit should refer them for further investigation/analysis. Internal risk rules and risk engines can facilitate the selection of cases for further investigation, while other data and risk analysis methodologies, including through the use of artificial intelligence, can also aid in identifying potential cases for review. For instance, the detection of taxpayers making substantial payments, such as property purchases from offshore entities, can prompt a more in-depth analysis to evaluate potential tax evasion risks.
- **Audit Referrals:** During ongoing audits, auditors may forward cases whenever they discover indicators of a suspected tax crime.
- **Referral from Attorney-General:** In some jurisdictions, the Prosecutor or Attorney General may have the powers to order than an investigation be opened (for example following a public scandal, whistleblower report, etc.).
- **Referrals from financial intelligence units (FIUs):** FIUs (which are primarily responsible for detecting money laundering based on reports from banks and other reporting institutions) often have analysts specialised in detecting tax crime risks. In some jurisdictions, the tax administration may have direct access to these databases, or the FIU may share such reports spontaneously or upon request (see also section 11)
- **Domestic inter-agency referrals:** Depending on legal gateways, other domestic tax and/or financial authorities may report or share information for further analysis by the tax crime investigation authority (see also sections 11-13 on domestic inter-agency co-operation)
- **Cross-border referrals:** Depending on the underlying mechanism for international co-operation, foreign tax and other financial authorities may be able to report or share information with their foreign counterparts (see section 20 on international co-operation for more detail).
- **Whistleblower reports:** Whistleblowers can be an important source of insider information within both public and private sector organisations, identifying and reporting tax and other financial crimes that would otherwise be difficult to detect (see section 14 for more detail).

Case review and selection

Following a referral, it is critical that cases are reviewed and selected for investigation through a structured and transparent procedure. The TCIM should include:

- Details of the person(s) and/or team responsible for conducting a case review;
- Criteria for case selection (i.e. specific indicators or red flags to determine whether the case is appropriate for criminal investigation). These may include:
  - *Actus reus* (an act or omission constituting a tax crime has occurred)
  - *Mens rea* ((the act was performed with intent and knowledge)
- The amount of undeclared or unpaid tax (particularly where legislation has a threshold approach for tax crimes).
- Procedures for case selection, including:
  - Any internal approvals or review processes (e.g. by senior leaders and/or an internal case selection body/committee, or prioritisation strategy);
  - Documentary requirements (e.g. a report outlining the reasons why a criminal investigation is necessary or proposing alternative actions that may better address the identified risks).

Case allocation

Once a case is selected for investigation, the manual should outline the procedures for how the case will be allocated to a particular team, unit, and/or individual for investigation and who has ultimate responsibility for the assignment of a case. Case allocation should consider a range of factors, including the experience of the team members, complexity of the case, and current case load.

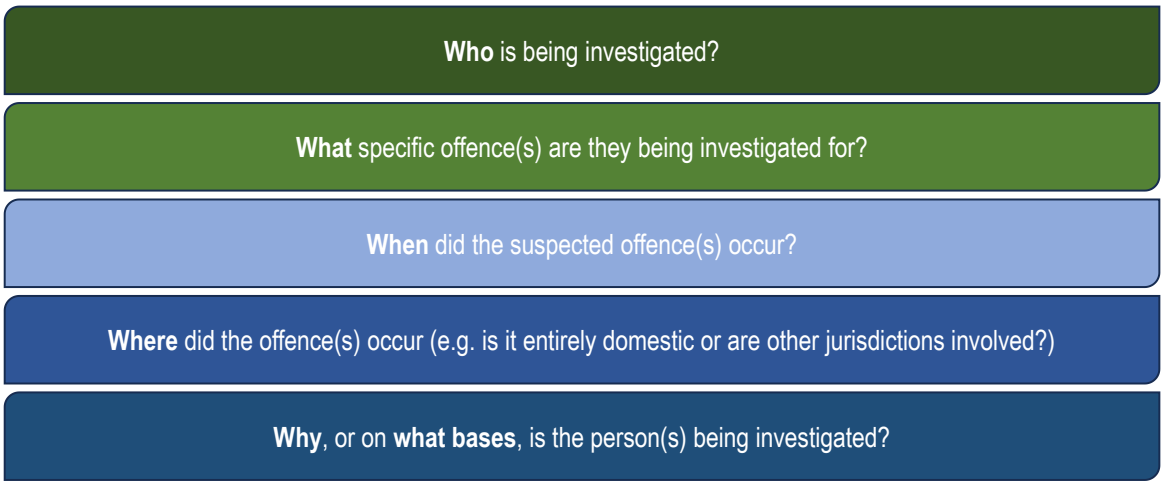
5 Case planning

Once a case is allocated to an investigation team, case planning is critical to ensure that both the investigator and the investigation stay on track. By adhering to a carefully crafted plan, the investigator can effectively co-ordinate different facets of the investigation and facilitate seamless co-ordination within the team and with relevant parties. While criminal investigations can often change course as new evidence comes to light, a well-prepared investigation team will be much better placed to make rational and informed decisions when it comes to adapting the case plan. To that end, an effective TCIM should prescribe planning activities and include templates to document and periodically review a case plan as it progresses. The below sections outline key elements of an effective case plan.

Case direction

Once a suspected crime has been referred for investigation, the core objective is to determine the theory of the case. At a basic level, the investigation team needs to define the who, what, when and why of the case, namely:

Figure 5. Setting the scene: Defining the case parameters



Source: OECD (2025)

Defining these parameters is a good rule-of-thumb for ensuring an investigation remains relevant and stays on track to achieve its ultimate objective. As more information and evidence is gathered, decision making

will become more refined allowing investigators to focus their attention on the most relevant leads and/or expedite decisions to progress or to close the case and redirect resources elsewhere (i.e. if it becomes clear that the initial suspicions were unfounded). These parameters can also be complemented by insights from internal legal departments and officers who may ultimately prosecute the case, who can draw on their experience on legal changes and judicial precedent to help guide the "how" any alleged offences could be proven to the standards required by the courts.

Mapping and prioritisation of actions

Case planning is critical for mapping out all stages of an investigation and allows the prioritisation of actions that are time sensitive. For example, where a case has criminal acts committed over several years, there may be relevant third-party information that is subject to mandated record-keeping time limits, (e.g. bank statements and transaction instructions) that could no longer be available if not obtained within these time limits. Equally, where information relates to offshore bank accounts, investigators will have to factor in the time to request mutual legal assistance and/or exchange of information from the foreign jurisdiction (see section 20 on international co-operation).

Actions should also be prioritised to maximise potential yield. For example, where there is suspected evidence that may be at risk of tampering or destruction, circumstances may necessitate the execution of a lawful search warrant without notice. However, doing this may also notify the suspect that they are under investigation and therefore the timing of any covert information gathering should take place prior to this action.

This demonstrates how important it is that the investigation team not only identifies the information and evidence it believes may exist, but also considers where that evidence is, how it will be obtained, and the consequences of undertaking the chosen information-gathering exercise.

Resource identification and co-ordination

Central to the planning process is the identification of required resources. For example, where covert surveillance is required, the investigation team should map out the processes and timelines required to obtain necessary approvals. Processes that are conducted by specialist teams within the organisation or by another domestic agency will also require the investigation team to engage with these counterparts early and co-ordinate with them, including to assist them with their planning and operational requirements to ensure the action is optimally executed. At a high level, resource planning should consider:

- Who are the targets of the investigation?
- Who may have information about the suspicions and what is their relationship to the suspects?
- What are the suspicions and what information is required to confirm those suspicions?
- What resources or processes will be needed to obtain that information?
- What agencies need to be engaged or consulted?
- Are there activities that need to be conducted covertly prior to notification?
- What is the anticipated lifespan of the case?

Regular review and recalibration of investigation plan

Case planning should also include periodic reviews to monitor progress and direction as well as evaluate the continued viability of success as new information comes to light. Tax crime investigation agencies should consider implementing periodic panel case reviews comprised of diverse individuals. Some groups to consider include:

- Department superiors to which the case team report directly to provide management with case oversight;
- Superiors from other departments within the agency on a rotating basis to provide alternative insights and fresh perspectives to mitigate against groupthink;
- Subject matter experts who have relevant internal knowledge and experience;
- Other key stakeholders such as prosecution and asset recovery counterparts to co-ordinate functions.

Components of the case plan

Table 1 below, contains a non-exhaustive list of a series of useful topics to include in a case planning document. These are indicative only and jurisdictions should adapt these to meet their domestic context. Any case plan should be considered a live document to be updated and adapted as new information is obtained and new or revised actions/timelines are required.

Table 1. Core elements of a case plan

Element	Description
Taxpayer Information	Identifying information that ensures the suspect is uniquely identifiable for example, taxpayer name, tax identification number, date of birth, etc.
Case background	Brief summary of the background information that prompted the investigation as well as any known relevant facts that are supportive of pursuable criminal risks being present.
Previous interactions with tax authorities and/or law enforcement	Any relevant interactions with the tax authority and/or law enforcement such as compliance history, previous lodgement reviews or audits and inbound correspondence with the tax authority such as updating any tax accounts or information as well as interactions with call-centre support. Similarly, any relevant interactions with law enforcement or available intelligence pertaining to the suspect, including any listing on registers such as firearm licences or sanctions lists.
Related entities	All entities with known or suspected connections to the taxpayer, such as corporate entities in which they hold official positions or shares in, partnerships to which they are a partner or trusts of which they are beneficiaries. Further, any known natural persons who are their authorised representatives, such as lawyers or powers of attorney as well as other suspected co-conspirators.
Detected risks & suspected offences	Details of the potential risks identified as well as the relevant legal offences.
Related crimes suspected	Details of any other suspected related criminal behaviour that may be beyond the mandate of the tax crime investigation authority, as well as if any referrals regarding these suspicions have been made to the relevant authorities to encourage a whole-of-government approach to disrupting criminal behaviours.
Tax periods	Which tax periods will be in the scope of the investigation, taking into consideration any years that may have expired due to applicable statutes of limitations.
Known and suspected sources of income	The types of income previously reported by the taxpayer in tax lodgements as well as other suspected sources of income (both licit and illicit).
Estimated size of risk	What is the estimated magnitude of amounts involved, including omitted assessable income, non-allowable deductions claimed, withholding amounts not remitted, etc., as well as associated resulting tax liabilities, penalties, fines and accrued interest, as applicable.
Scope & objective of investigation	Determining the potential charges to be investigated.
Anticipated information gathering	Initial information gathering measures to further assess the identified risks, including considerations of both covert and overt actions and how these will mitigate evidence destruction, as well as any ancillary resources required, such as police support, that needs to be considered and co-ordinated. This can include a list of

	(1) Key documentary evidence required or suspected to exist, where this is believed to be located, and how it can be lawfully obtained. (2) Key individuals to be interviewed. (3) The potential need for international co-operation to access either of the above.
Known assets and measures to secure them	Identifying any known assets, including details of other joint owners or encumbrances such as mortgages so that provisional asset recovery measures (e.g. freezing and seizing) can be considered from the outset to best secure the collection of outstanding revenue and associated criminal proceeds. Common assets include bank accounts or other financial products such as shareholdings and term-deposits, real property, motor vehicles, sea and aircraft, collections, luxury goods and precious metals.
Estimated case-cycle time	An estimate of the time to be devoted to the investigation to keep staff on track and monitor resource allocation.
Manpower required	Delegation of officers and their respective roles in the investigation team to monitor human resources allocated to the case.
Challenges and threat identification	Detailing of any anticipated challenges or threats to the investigation's success so that mitigation and other alternative strategies can be considered to address these.
Attachments	Any intelligence referrals, initial profiles, or other relevant documents pertaining to the case should also be attached as annexes to the case plan.

Source: OECD (2025)

6 Notifying the suspect they are under investigation

Some jurisdictions may require that a person is formally notified that they are suspected of having committed a criminal tax offence and are under investigation in relation to that offence. In other jurisdictions, it may be permissible to conduct covert investigations where the suspect is unaware that they are under investigation. Regardless of the situation, an effective TCIM should:

- Prescribe when and how suspects should be advised that they are under investigation.
- Detail any measures to mitigate against asset dissipation. For example (and as noted in section 15 below) measures should be taken, where available and appropriate, to identify, freeze, and seize any assets that are likely to be the proceeds of crime at an early stage to secure them for possible confiscation at a later stage.
- Outline measures to prevent the flight of the suspect. For example, some jurisdictions may have powers to require a suspect to surrender his or her passport prior to notifying them of an investigation and/or issuing formal charges. Such measures that restrict a person's freedom of movement are serious, therefore a TCIM should be very explicit as to when and how such measures can be employed.
- Describe the fundamental rights afforded to persons suspected of tax crimes and how these should be applied**.** See section 24 for more details in suspects' rights.

7 Powers to identify assets, gather information, and obtain evidence

Tax crimes by their very nature often involve the concealment of income or assets for the purpose of evading a tax liability. This can be done by laundering the illicit funds through shell companies, or the use of offshore accounts to conceal the true beneficial owners of the assets in question. The speed with which criminals can now operate and move funds across multiple borders makes it increasingly challenging for law enforcement authorities to keep pace. To that end, it is critical that, while ensuring suspect's rights and confidentiality safeguards, governments have at their disposal a full range of powers to enquire into the financial affairs of persons suspected of criminal activity. This is important for identifying the extent of criminal networks; scale of criminality; identifying and tracing criminal property or corresponding value; and developing evidence which can be used in criminal and confiscation proceedings (see Recommendation 30. (FATF, 2012-2025[7]).

The nature and extent of powers available to criminal tax investigators will vary depending on which agency has responsibility for conducting investigations. Some powers may be held directly by the agency mandated to conduct the tax crime investigation, whereas others may require the investigators to request the assistance from another agency or obtain a court order from a judge. For example, in the process of conducting a thorough financial investigation, it is anticipated that investigators would rely heavily on financial intelligence from FIUs, as well as financial information that can be legally compelled financial institutions (including banks); virtual asset service providers (VASPs), and non-financial businesses and professions. The information held by these institutions (e.g. account statements, transaction records, KYC information) is relevant for building the profile of the accused and gaining a comprehensive understanding of their assets and liabilities.

To avoid misuse of powers (whether deliberate or accidental) and ensure that information gathered can later be used as evidence in court, it is critical that each jurisdiction establish clear regulations and policies in accordance with domestic law. Compiling all relevant laws and regulatory processes in place within the TCIM will help raise awareness of the array of powers available to an investigator, particularly with regards to less routine powers, and ensure the correct and timely application of these powers in practice.

Common powers, techniques, processes, and resources used by criminal tax investigators to gather intelligence, trace assets, and ultimately obtain evidence that can be used in court are listed below and outlined in more detail throughout this guide:

- **Powers to obtain documents from third parties**: For example, routine and non-routine third party notices (see section 8).
- **Covert information gathering powers:** Examples include telecommunication and mail intercepts, public and private surveillance and undercover operations (see section 9).
- **Use of open intelligence sources:** For example, social media monitoring, web scraping tools, blockchain analysis, geo-location, dark web, public records, etc. (see section 10).

- **Domestic inter-agency reporting and information sharing:** Ensuring that there are legal and operational mechanisms in place to support reporting and information sharing between tax and other financial crime authorities (e.g. financial intelligence units) is essential to combatting tax crimes and tracing illicit financial flows (see section 11).
- **Use of enhanced forms of inter-agency co-operation:** For example, joint intelligence centres, joint investigations, parallel civil and criminal tax investigations, secondments and co-location of staff (see section 12).
- **Access to government databases and registers:** For example, registers of companies, beneficial ownership (BO), trusts and other fiduciary arrangements, motor vehicles, real estate, etc. (see section 13).
- **Implementing an effective whistleblower regime:** Whistleblowers can play a key role in uncovering tax and other financial crimes that would otherwise be difficult to detect and enhance the success of a prosecution (see section 14).
- **Powers to search property and seize evidence and criminal proceeds:** Ensuring law enforcement authorities have effective powers to search and seize physical and digital evidence, including the instruments and proceeds of crime is critical to successful case outcomes (see section 15).
- **Asset recovery powers:** The ability to freeze (including rapid freezing), seize, and ultimately confiscate assets is crucial to ensuring that criminals do not profit from their offending (see section 17).
- **Powers to conduct interview and inquiries:** Both tools are an essential means of obtaining intelligence and evidence for use in criminal tax investigations (see section 18)
- **International co-operation:** It is critical that tax and other law enforcement agencies can engage with their foreign counterparts to obtain evidence and trace assets. Co-operation can take place through both informal mechanisms and networks as well as formal co-operation (i.e. through use of bilateral or multilateral treaties or memoranda of understanding (see section 20).
- **Financial analysis:** Tax and law enforcement authorities need to be trained on both direct and indirect methods of proof in order to be able to effectively analyse financial data and reconstruct a taxpayer's overall finances (see section 22).

When developing a TCIM, jurisdictions should include *all* powers available in their domestic context. Every information gathering power included in the part of the TCIM, should be accompanied by:

- A general description of what the process is, what it is used for and in what instances the process is both appropriate and effective to use;
- A reference to the relevant legislation that confers the power and to any laws, regulations, or internal policies that delegate and regulate the use of the power;
- An explanation of what is required to lawfully exercise the power, including approvals required and how to correctly document any decision making to demonstrate that the actions taken were justified and due process was followed.
- Links to any templates for documents and applications that may need to be completed or submitted, or directions where these could otherwise be obtained;
- Contact details of a nominated internal subject-matter expert on the process who can be contacted for further information or clarifications.

It can also be useful to include tips from any recent examples of where the power was used (with or without success) and the drivers that determined its success or failure. Table 2 sets out an example of how a power could be set out in a manual.

Table 2. Example process template for issuing a notice to produce information and documents

Purpose	To obtain information and/or documents, including digital media, from a natural or legal person.
Relevant Legislation	Section 49, Evidence Act 2000.
Required approvals	An authorised officer must review and sign notices. (Link to information sheet of *Who is an authorised officer?*)
Duration	30 days is the generally prescribed turnaround period for recipients to respond to the notice.
Relevant templates	• *Template notice for issue to natural person.* • *Template notice for issue to legal person.* • *Templates for specific type of documents requested, such as annexes related to financial records, communications, notes etc.* Link to Walkthrough document and FAQs available on intranet
Required recordkeeping	• Upload signed notice to Case Management System (CMS) • Load and complete Outbound Notice reporting activity in Case file on CMS. • Load and complete Outbound Notice response activity in Case file on CMS
Subject Owner	• A list of internal Notice Request Specialists for assistance preparing your notice is available *here*
Recent Developments	• Court dismisses key evidence as inadmissible after hearing Notice to Produce issued to accountant was not signed by an Authorised officer – Link to news article • Match Fixing Unit advises that Sports Betting Operators can provide geolocation and IP address data for bets placed online.- Link to intranet article.

8 Power to obtain documents from third parties

Requesting documents from third parties such as banks and other financial institutions is a fundamental step in any financial crime investigation. An investigator may be empowered, either directly or indirectly, to request information and documents from a third-party, or by detailing these in a legal document such as a warrant, notice to produce, or subpoena. TCIM should both educate and create awareness among investigators of the breadth of information held by both routine and non-routine third parties, how these may be used in an investigation, and the correct process to follow to obtain the documentation.

Routine third-party notices

Use of routine third party notices to obtain financial information

In criminal tax investigations, notices are routinely issued to third parties who are not complicit in the commission of a crime and are willing or legally compelled to assist law enforcement by complying with requests or orders for information and documents. These types of third parties are often large enterprises, both domestic and offshore, such as financial institutions (e.g. banks); share trading and virtual asset service providers; property and asset registers; accounting firms or cloud accounting software providers; and gambling services (e.g. betting companies and casinos).

Third-party notices are a means of obtaining financial information. Banking institutions hold a wealth of information about a person's financial affairs and monitoring account activity can help investigators analyse lifestyle indicators and spending patterns, detect unexplained wealth, reveal financial troubles, and identify associations with other individuals to/from whom payments are made and/or received. Accounting monitoring can be very useful in identifying the source of illicit funds, linking transactions to suspected offences, tracing IFFs, and for preserving assets.

These types of third parties have their own confidentiality requirements and commitments to protecting the privacy of information they hold about their customers that necessitates a legal notice or warrant to be served upon them so they can lawfully provide the requested information to law enforcement. Larger institutions tend to have dedicated staff or teams responsible for compliance with such notices and liaising with law enforcement authorities and typically pose a relatively low risk of jeopardising an investigation by notifying a suspect that they were the target of such a notice unless there is a legal obligation to do so.

To ensure the efficient use of routine third-party notices, a TCIM should include procedures and where possible templates that can be easily adapted to the recipient of the notice. The TCIM should also include advice on how to prepare a notice to ensure it meets legal requirements and contains sufficient information so that it elicits a complete and accurate response from the recipient in the first instance. The TCIM may

specify whether and how to obtain legal advice or to seek the involvement of prosecutors or the judiciary in the issuance of notices, as may be required under domestic law.

Other types of information available from routine third parties

In addition to bank statements and detailed records of transactions, financial institutions may also retain information and documents such as CCTV footage from both ATMs and in-branch interactions; geolocation and IP address data for online transactions; supporting documents such as assets owned and proof of identity used to open accounts and apply for other financial products such as home loans; as well as information they have collected from conducting their own investigations for Know Your Customer (KYC) purposes and compliance with other regulatory requirements such as AML/CFT legislation. This can be critical for tracing assets and obtaining evidence.

In some instances, particularly where an investigator is seeking atypical information or where they are unsure if a third-party has a particular type of document in their possession, the manual should encourage the investigator to contact the third-party recipient in the first instance to ensure the information exists and if so, how to obtain it. This can help to minimise the burden on the recipient whilst providing them with advance warning of the request. This will help avoid an incomplete or unintended responses, minimising the need for additional requests and promoting a better relationship between the two parties.

Directory of third-party notice recipients

As part of its TCIM, an agency may consider developing and maintaining a directory with the various routine third-party notice recipients in their jurisdiction and how to best interact with them. For example, one bank may prefer to be sent their notice by letter, whereas another may have a secure digital file transfer platform to receive and respond to requests. At an aspirational level, agencies should seek to build tailored relationships with these routine third parties, that both takes into account their individual preferences and makes it as easy as possible for the recipient entity to clearly understand and respond to the request in an accurate and timely manner.

As noted above, larger institutions tend to have dedicated staff for such notices. A directory of routine third-party contacts could include:

- Where to address the notice;
- Preferential methods of serving the notice;
- A list of the potential information and documents that the entity can provide, including details of how long that information is retained by the entity, as well as what specifics they require in the notice to both easily and accurately obtain the exact evidence sought as well as compliantly provide that information;
- Any entity specific terminology or details that can increase the accuracy of a request. For example,
    - When requesting transaction tracing details, a bank may suggest the notice refers to these by a particular phrase, such as ‘remittance instructions’ and require the transaction ID, the date, account number, and direction (credit or debit) of each transaction to most accurately provide the correct response to the requesting agency.
    - Similarly, a bank may also suggest some limitations, for example a maximum of 20 transactions for tracing per notice, so to encourage an efficient and accurate response by its staff who prepare the entity’s response to law enforcement.
- Links to any preferred templates that have been developed in collaboration with the third-party recipient, preferred method of response, and any technical requirements for the production to be included in the notice to enable internal analysis once the response is received (e.g., xlsx format).

- A focal point within the third-party institution who can be contacted for further information.

Non-routine third-party notices

Other third-parties who may have relevant evidence require more strategic consideration before issuing a formal request for the documents in their possession, for example a related party of the suspect, such as a family member or business partner. In the first instance, a manual should advise an investigator to consider the following criteria before drafting a notice to a non-routine third-party:

- Is it appropriate to approach the third party at this point of the investigation?
- Is the recipient potentially complicit in the crime?
- What is the likelihood that the recipient has the information and will be co-operative?
- Can the desired evidence that they possess be obtained elsewhere?
- What is the likelihood the recipient may notify the suspect they are the target of a criminal investigation?
- How burdensome is the request upon the recipient and can it be made easier for them to comply?

For instance, where an investigator ultimately determines that a notice to produce documents to a non-routine third party, the TCIM should provide guidance on how to do so including:

- Use clear and exact language that makes it easy for the third party (who may not be familiar with the corresponding legal process) to understand their legal obligations to comply with the notice and the consequences of not doing so.
- Be mindful that a notice to produce information and documents can be both burdensome and stressful for non-routine third parties and seek to maintain a positive working relationship at all times (particularly where the third party is not suspected of having committed an offence).
- Where the circumstances permit, contact the third party (or their counsel) in advance of issuing the notice to inform them of its purpose and their lawful obligation to comply.
- To minimise the burden on them, seek to understand what information and documents they have in their possession to discern what may be relevant and irrelevant to the investigation before drafting the notice.

9 Covert information gathering processes

Covert information gathering powers can be strategically used, particularly in the earlier stages of information gathering, to gather intelligence and evidence about the suspected criminal behaviour and its *modus operandi* without alerting the suspect that they may be the target of an investigation. When effectively deployed, covert information gathering can gather both inculpatory and exculpatory evidence about the target, as well as identify any co-conspirators or accessories to the crime. This allows law enforcement authorities to accurately concentrate their efforts towards the right targets and consider the possibility of early exit where the suspected criminal behaviour is not confirmed.

Covert information gathering mechanisms can also be useful for the early identification and tracing of criminal assets, such as those effectively controlled by the suspect even if held in the names of others, as well as additional locations for further surveillance activity or subsequent search later in the investigation. While covert investigative methods provide significant advantages to law-enforcement, their intrusive nature often necessitates additional levels of approval, for example, from an agency director, Tax Commissioner, the prosecution or the courts.

Common covert information gathering methods include:

- Telecommunication intercepts including the accessing of stored electronic communications and data from telecommunication service providers;
- Mail intercept;
- Surveillance both in public and in private, including the use of devices that track movement, data usage, record video or audio, or any combination of these;
- Undercover operations both in-person or digitally over online platforms.

The emergence of the dark web, cryptocurrencies, and other virtual assets, and their subsequent utilisation in tax and other financial crimes has, in many jurisdictions, led to the introduction or broadening of legal powers traditionally reserved for more grave crimes like terrorism or child abuse. As of 2019, VASPs are required to be brought under the AML/CFT regulatory regimes of jurisdictions, meaning that information may be sought from these entities as it would be from other financial institutions or non-financial businesses (See FATF Recommendation 15, preventative measures with respect to new technologies, including VASPs) (FATF, 2012-2025[7])). Similarly, an increasing number of jurisdictions have announced their intention to commence exchanges under the Crypto-Asset Reporting Framework (CARF), which extends the automatic exchange of information of tax purposes to the crypto-asset sector, in 2027 (OECD, 2024[8]).

In jurisdictions where such powers are now available to tax crime investigators, they may be unaware of their availability and potential application. Similarly, their superiors may be hesitant to approve such courses of action where the approval process is not well known. Accordingly, their inclusion in the TCIM should both create awareness of the existence of these powers, how to use them, and provide reassurance that encourages their use in appropriate situations.

Box 7. Successful use of covert surveillance in Operation Elbrus in Australia

From early 2014 a group of offenders conspired to skim taxes that were to be paid from Australian workers and companies to the Australian Taxation Office (ATO) for their own benefit. In summary, the core group of the offenders conspired to funnel workers' payroll through various 'subcontracting' companies and then siphon off, for their own benefit, the money that was to be paid to the ATO as Pay as You Go Withholding Tax (PAYG tax) and Good and Services Tax (GST).

The conspirators planned for the parent company to appear legitimate while the subsidiary 'subcontracting' companies would process the payroll and retain the PAYG and GST liabilities. These subsidiaries had straw directors who were installed to conceal that the entities were in fact controlled by the conspirators. The agreement was that these subcontracting companies would be periodically phoenixed, with new subsidiaries created, to avoid ATO attention and allow the scheme to continue. Between 2014 and 2017, the conspirators were able to collect over $140 million in PAYG and GST and caused a loss to the Commonwealth of over $105 million.

Unknown to the offenders, in 2016 a joint investigation named Operation Elbrus was initiated by the ATO and the Australian Federal Police (AFP) as part of the ATO-led Serious Financial Crimes Taskforce (SFCT), which brings together 9 Commonwealth agencies to form a whole-of-government approach to tackling the most serious forms of financial crimes. The investigation was substantially assisted by the AFP's use of covert recording devices at key offices used by the offenders as well as intercepting telephone conversations which were able to reveal to investigators the syndicate's criminal methods. In addition to gathering key evidence about the criminal activity, the conspirators themselves in a covertly recorded conversation commented on the size of their fraud, noting that if authorities ever fully uncovered their operation that "it would be the biggest tax fraud in Australia's history."

When investigators determined they had gathered enough evidence, they co-ordinated to simultaneously arrest the suspected co-conspirators and execute search warrants in their homes and business premises. Over AUD 15 million in cash as well as an additional AUD 1 million located in a bank safe deposit box, 25 vehicles, 12 motorbikes, 18 residential properties, over 100 bank and share trading accounts, two aircraft, firearms, jewellery, art and vintage wine were seized by authorities as part of asset recovery action.

In total, over 70 hours of surveillance recordings as well as 28,000 pages of documentary evidence were used by the Commonwealth Director of Public Prosecutions (CDPP), also part of the SFCT, in addition to the calling of expert witnesses from the AFP and ATO specialising in tax analysis and forensic accounting to successfully convict 14 individuals involved in the tax fraud and conspiracy to launder the proceeds of these crimes.

Source: Australian Taxation Office, Australia (2025).

10 Open source intelligence

Open-source intelligence refers to the process of gathering and analysing information from publicly available sources. This can be a powerful tool for investigators in both preventing and combatting tax crime and tracing and recovering assets. This is an area where artificial intelligence tools may have an increasing role to play over time. The TCIM should identify wide-ranging open intelligence sources that could be useful for criminal tax investigators, including:

- **Social media monitoring:** Criminal investigators may have access to specialised tools for monitoring or social media to detect potential tax crime threats or risks, collect evidence in ongoing investigations, and identify connections between individuals and/or criminal networks.
- **Automated web scraping tools:** These tools can help investigators gather large datasets from broad ranging online sources such as public records and news articles, advertising platforms, forums and blogs.
- **Blockchain analysis:** Investigators in many jurisdictions will also have access to tools to analyse suspected crimes involving crypto currencies. For example, private-sector solutions can help with identifying persons sending and receiving crypto-currency and their transaction histories, helping to trace illicit financial flows.
- **Geo-location:** Open-source intelligence tools can help law enforcement geo-locate suspects and witnesses through use of location data and satellite imagery.
- **Dark web investigations:** Law enforcement authorities may also have access to tools that enable them to identify and monitor illegal activities taking place on the dark web.
- **Public records:** Investigators can also leverage publicly available government sources such as registers of real estate, beneficial ownership (BO), professional licensing information, vehicle registration data, etc. (see also section 14 on access to government databases).

11 Operationalising a whole of government approach: Domestic inter-agency reporting and information sharing:

Beyond the tax administration, various government agencies hold a wealth of information that can be critical for the investigation of tax crimes and recovery of assets. Moreover, in many cases, criminals that commit tax offences may also be under investigation for other crimes, such as money laundering or bribery and corruption, or breaches of regulated activities, such as the rules that apply to financial and professional service providers. For this reason, jurisdictions are recommended to adopt a whole-of-government approach that supports effective reporting, information sharing and co-operation among tax authorities, customs administrations, financial regulators, AML/CFT authorities such as FIUs, the police and specialised law enforcement agencies, anti-corruption authorities and the public prosecutor's office (OECD, 2021[6]).

The critical importance of information sharing was also reflected in the FATF's 2023 Recommendation related to asset recovery, which emphasizes the potential interactions between competent authorities responsible for investigating money laundering, predicate offences (including tax crimes), and terrorism financing, on one hand, and tax administrations, on the other.[1] The Standard states, in pertinent part: "Countries should enable their competent authorities and tax authorities to cooperate and, where appropriate, coordinate and share information domestically with a view to enhancing asset recovery efforts and supporting the identification of criminal property. This could, in appropriate cases, where there is a tax liability, support the recovery of such liabilities by the tax authorities." (see Interpretative Note to Rec 4, (FATF, 2012-2025[7]).

To support effective co-operation in practice, a TCIM should outline the legal and operational mechanisms for information and intelligence sharing between different tax and financial crimes agencies for investigative purposes, including:

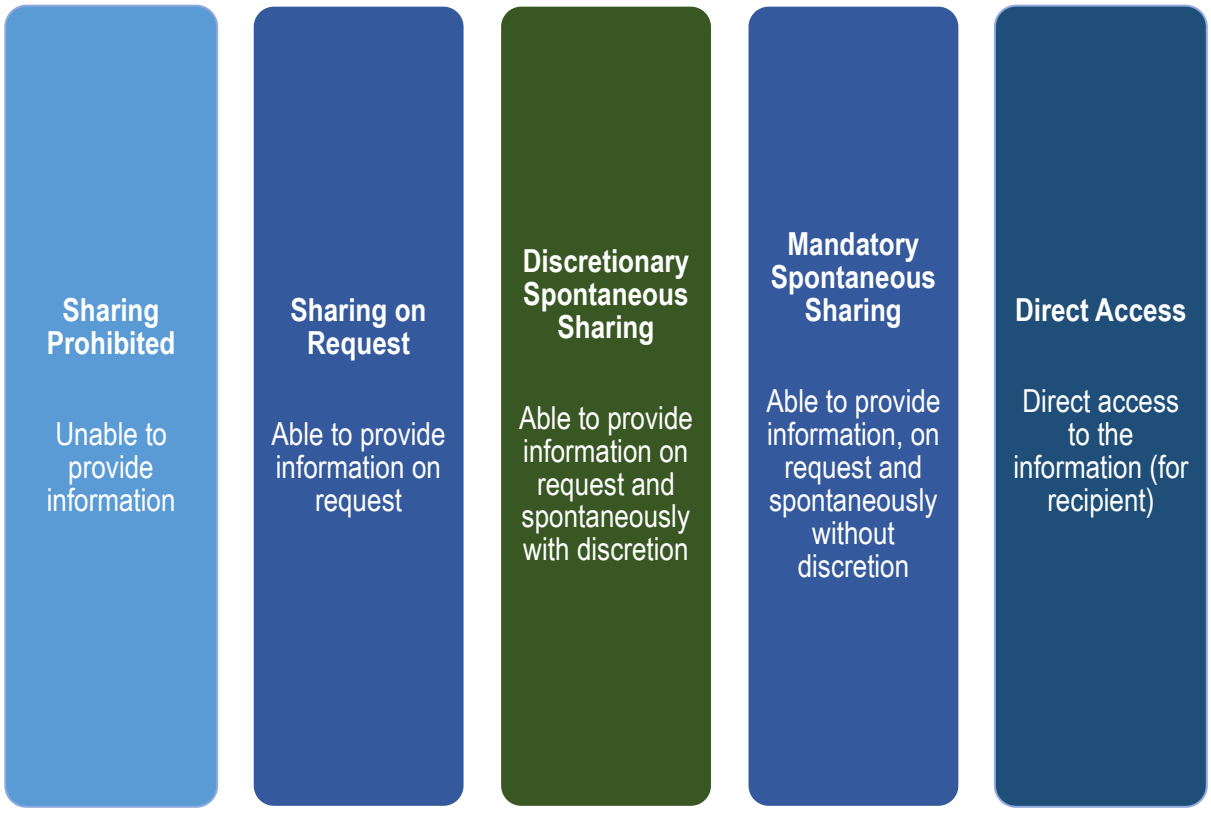
- The underlying legal bases for reporting of suspected crimes between different tax and financial crimes agencies (e.g. whether reporting and information is mandatory, discretionary, restricted, or prohibited).

[1] See FATF Recommendations (https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf), Interpretive Noted to Recommendation 4 (Feb. 2025 ed.) (confiscation and provisional measures),

- The underlying legal bases for sharing information related to suspected crimes between different tax and financial crimes agencies (e.g. the law provides for spontaneous sharing (and whether mandatory or with discretion); whether information can only be shared upon request (with or without discretion); or whether sharing is prohibited (see Figure 6 below).
- Operational mechanisms in place that govern when and how this reporting and information sharing should take place (e.g. descriptions of the process for reporting/sharing information and/or links to any MOUs, co-operation agreements in place, etc.).
- Contact points for requesting and/or sharing information across agencies (to be updated on an ongoing basis).

To help guide jurisdictions with this exercise, the figures and boxes set out below present common information sharing models; the importance information held by FIUs; information sharing procedures within Italy's *Guardia di Finanza*[2], as well as a range of useful resources reflecting international best practices with respect to reporting and information sharing between domestic agencies responsible for combatting tax and other financial crimes.

Figure 6. Models for domestic information sharing between agencies responsible for combatting tax crime and other financial crimes



Source: OECD (2025)

[2] Guardia di Finanza is an Italian force with military status and nationwide remit for investigating financial crime, including tax crime.

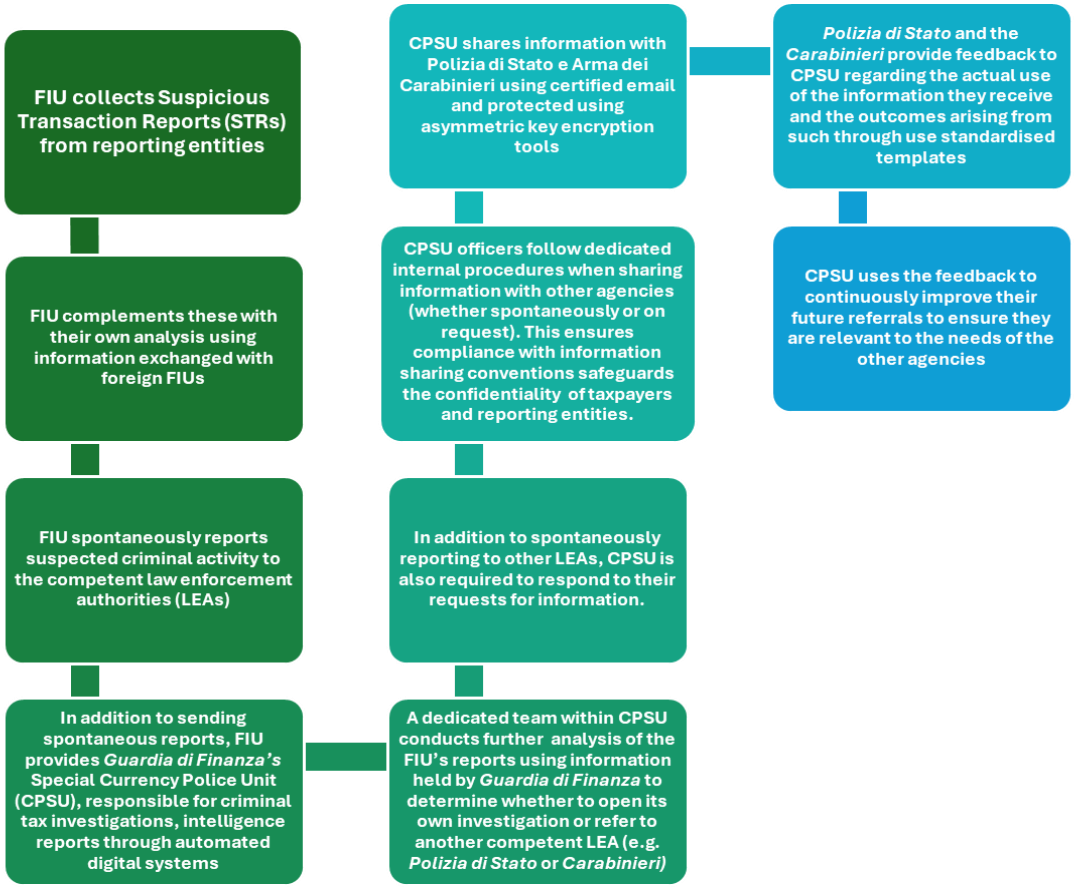
Box 8. Spotlight on information held by Financial Intelligence Units

Financial intelligence refers to the product resulting from financial analysis or work done to add value to available and obtainable information. Financial intelligence should be available through the jurisdiction's FIU, upon investigator request or via spontaneous dissemination. In some jurisdictions, law enforcement may also have direct access to certain financial intelligence. Financial intelligence comprises or builds upon filings made by the private sector and other entities which are required to submit to the jurisdiction's FIU suspicious transaction reports (STRs) and other reports, such as Currency Transaction Reports and International Wire Transfer Reports as required domestically, for AML/CFT purposes. In the case of the FIU, financial intelligence is the product of its operational (case specific) and strategic (risk and trend) analysis functions. FIUs are also able to seek additional information from reporting entities, which enriches their products and thus provides valuable leads to tax investigators (see Recommendation 29 (FATF, 2012-2025[7])). Tax investigators and law enforcement are the target audience and main consumers of financial intelligence from the FIU, but this is lead information only, and evidence for use in court must later be corroborated and obtained through a different process. Financial intelligence can be a valuable, even necessary, step in the investigative process, including for mapping the flow of funds related to an offence and identifying and tracing assets. It can also point investigators to the need to obtain specific financial records for use as evidence admissible in court or to take additional investigative steps.

Understanding and using the information available from reporting entities themselves and the financial intelligence products available from the FIU is essential for tax investigators to carry out their functions. These two major sources of information are crucial to detect, investigate, and prosecute tax and other financial crimes. The TCIM should clearly identify when and how such sources can be utilised and the processes and tools for doing so. The ongoing financial investigation may also reveal the existence of funds, accounts, and other products which should be frozen or restrained with a view to confiscation (see section 17). Consequently, the TCIM should identify available avenues for the restraint of financial assets held by banks and other entities, including virtual assets.

Source: Financial Action Task Force (2025).

Figure 7. Inter-agency reporting in Italy



Source: Guardia di Finanza (2025)

Box 9. Useful global resources on domestic reporting and information sharing between tax authorities and other financial crime authorities

A core component of an effective whole-of-government approach to fighting tax and other financial crime is inter-agency trust. In order to assist jurisdictions in assessing and improving their level of maturity as regards trust among financial crime authorities, in 2023, the OECD, in collaboration with the South African Revenue Authority developed two new tools:

The Inter-Agency Trust Maturity Model is a tool for jurisdictions to self-assess the level of maturity of their practices and processes for achieving and maintaining inter-agency trust; This can help them identify possible areas for improvement of their internal and cross-agency strategies. (OECD, 2023[9])

The Inter-Agency Trust Perception Survey may be used either before or after undertaking a self-assessment using the Inter-Agency Trust Maturity Model. The survey is intended to help tax and other financial crime authorities understand how they perceive each other. (OECD, 2023[9])

In addition to these tools, below is a (non-exhaustive) list of resources that provide comprehensive information on the legal, institutional, and operational, mechanisms that jurisdictions should have in place to support effective and efficient co-operation between tax and other financial crime authorities.

- Bribery and Corruption Awareness Handbook for Tax Examiners and Tax Auditors (OECD, 2013[10])
- Designing a National Strategy against Tax Crime: Core Elements and Considerations (OECD, 2024[4])
- Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes - Third Edition (OECD, 2017[5])
- Improving Co-operation between Tax Authorities and Anti-Corruption Authorities in Combating Tax Crime and Corruption. (OECD, 2018[11])
- Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors (OECD, 2009[12])
- Tax Crime Investigation Maturity Model (OECD, 2020[13])
- Taxing Crime: A Whole-of Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes (Cebreiro Gomez et al., 2022[14])

12 Enhanced forms of inter-agency co-operation

Beyond reporting information sharing, there are a range of other forms of co-operation that may be available to jurisdictions. The TCIM should describe all available mechanisms for inter-agency co-operation between tax and other financial crime authorities, including those responsible for the recovery of assets. For each mechanism/form of co-operation available in a jurisdiction, the TCIM should include:

- References to the underlying legal bases for the co-operation tool in use;
- The procedures and/or criteria for determining whether and what form of co-operation is most appropriate in a given case;
- Guidance for investigators on how to initiate use of the co-operation mechanism (e.g., how to send a request to another agency to launch a joint investigation);
- The process for requesting or responding to a request for enhanced co-operation from another agency;
- Clear procedures for how each co-operation mechanism will operate in practice (including links to any inter-agency MOUs that govern the operations between the agencies involved. Among others, the operating procedures should include:
  - Guidance on how to share case-related information between agencies;
  - A description of how consultation and co-ordination will take place in practice;
  - Policies on collecting and accessing information that may be used as evidence;
  - Guidance on questioning and obtaining statements from suspects, witnesses, and/or informants; and
- Policy on disclosure of information released to the public regarding cases.

Some common forms of enhanced co-operation available in tax crime investigations are set out below. For more detailed information on the benefits of these mechanisms and examples of how countries use them in practice, please refer to: *Improving Co-operation between Tax Authorities and Anti-Corruption Authorities in Combating Tax Crime and Corruption* (OECD, 2018[11]), *Effective Inter-Agency Co-operation in Fighting Tax Crimes and Other Financial Crimes - Third Edition* (OECD, 2017[5]) and *Fighting Tax Crime - The Ten Global Principles - Second Edition* (OECD, 2021[6]).

Joint intelligence centres

Joint intelligence centres are an effective tool for co-ordinating information gathering, analysis, and distribution across a number of agencies. By centralising these activities, countries can benefit from cost savings and more efficient use of operational information (i.e. case specific information and investigations relevant to more than one agency). Such centres also support with a jurisdiction's overall strategy for

fighting illicit financial flows through a broader assessment of risks and threats as well as the identification of trends through combined analysis of datasets held by different authorities. To be effective, joint intelligence centres need to be underpinned by laws that facilitate effective handling of intelligence across multiple agencies.

Joint investigation or operations

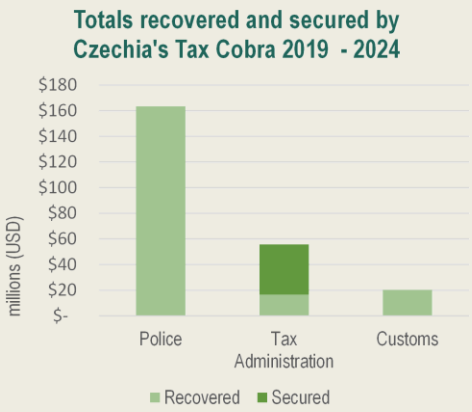
An effective whole of government approach to fighting tax crime relies on tax crime investigators having the ability to work with other financial crime agencies with a common interest in the case (e.g., anti-corruption authorities, money laundering investigators, asset recovery authorities etc.). In addition to reporting and sharing information with each other, joint investigation teams enable each agency to utilise a broader range databases and software tools, and to benefit from the experience of investigators with different backgrounds, skillsets, and experiences. Joint investigation teams can help avoid the duplication that can arise from parallel investigations and increase efficiency, particularly where they provide a legal basis for broader information sharing. Beyond information sharing, case strategies may be co-ordinated in appropriate cases, to include approaches to investigative steps, charging decisions, and asset recovery considerations. By working together in a complementary manner, tax and other financial crime authorities can ensure various forms of criminality are dealt with simultaneously, thus strengthening enforcement outcomes. Options for forming joint investigative teams should be covered in the manual, as well as any possibilities of working in a standing task force with authorities having overlapping objectives.

Box 10. Czechia's Tax Cobra strikes to preserve 16 billion Czech crowns

In 2014, Czechia established a whole-of-government tax crime strategy called Tax Cobra (*Daňová Kobra*) to combat tax evasion and tax crime in Czechia by combining investigators and resources from the National Centre for Organised Crime of the Czechia Police, the Financial Administration, and the Customs Administration. Tax Cobra does not operate as a centralised team or department, but rather it is a system of co-operation between the police, customs, and tax officials for the purpose of immediate information sharing within the legal framework, both at the national and regional levels, and through timely and effective co-ordination of procedures in tax and criminal proceedings to disrupt the criminal activity, protect the state budget, prosecute tax crime facilitators and recover the proceeds of crime.

Participating agencies in Tax Cobra meet regularly to discuss and address procedural issues that arise between agencies; share knowledge, identify new cases, and establish co-ordinated approaches in ongoing cases.

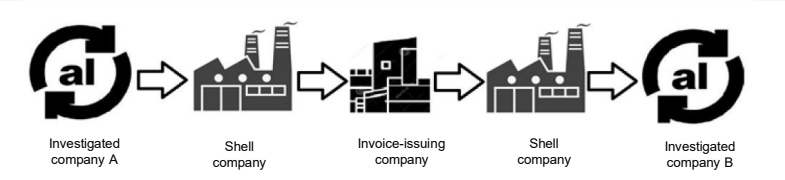
Tax Cobra measures its effectiveness by the amount of state revenue 'preserved', which includes amounts recovered from offenders through its asset recovery efforts as well as the amounts the tax administration prevents from being refunded to the offender. Since its establishment in 2014, Tax Cobra has preserved over 16 billion Czech crowns (approximately USD 696.5 million)* for the Czechia state budget.



Source: General Financial Directorate, Czechia (2025).
*Calculated based on average conversation rate for the years 2014-2024.

Box 11. Operation Metal Shield. A Co-ordinated Effort to Unmask Tax Fraud in Brazil's Thriving Aluminium Recycling Sector

Brazil boasts one of the highest recycling rates for aluminum cans globally, maintaining levels above 95% since 2004 and generating approximately USD1.23 billion annually. However, in 2021 routine tax audits revealed indicators of structured tax fraud within the aluminum recycling sector, resulting in substantial losses to various federal and state taxes, including social contributions, corporate income taxes, and value-added taxes.



To counter this, the Intelligence Co-ordination of the Federal Revenue Service (FRS) of Brazil (a specialised unit within the national tax authority) initiated in-depth intelligence and investigative actions to dismantle the scheme. These included the extensive cross-referencing of tax data, meticulous analysis of financial documentation, field operations and the diligent monitoring of suspicious financial transactions, enabling authorities to map the intricate network of irregularities.

As the investigations progressed, a collaborative effort involving the various federal agencies including the FRS, Police, Public Prosecutor, Attorney General, Treasury, and Economic Defense proved pivotal in combating this billion-dollar tax evasion that was undermining fair competition within the aluminum recycling sector. Throughout the proceedings, authorities worked in tandem to uncover sophisticated fraudulent schemes involving the systematic use of shell companies to simulate commercial transactions, generate fictitious tax credits, and obstruct the tax authorities' ability to trace illicit financial flows.

In October 2021, the joint investigation culminated in the simultaneous execution of search warrants at 61 locations which had the immediate impact of the implicated group acknowledging and ceasing the use of fraudulent invoices. Throughout 2022, the group engaged in joint meetings with FRS, Police, Treasury, and the Offices of the Attorney-General and Public Prosecutor with the aim of formally confessing their tax debts and seeking reduced criminal penalties. The tangible results of this joint operation included:

- USD 576 million in tax settlements under which 23 companies settled or arranged debt payment plans with negotiated discounts resulting in the swift recovery of substantial sums.
- USD 54 million in penalties and interest following confessions relating to the improper use of tax credits totaling over USD 41 million.
- Significant shift in compliance with the group declaring and paying over USD 14 million in taxes between October 2021 and January 2023, a substantial increase compared to previous years.

In the wake of this operation, the FRS remained vigilant, actively working to prevent other irregular competitors from gaining dominance in the market. This proactive and sustained approach led to two major new operations: "Operation Alumidas" in Mato Grosso do Sul and "Operation Scrap" in Rio de Janeiro, further reinforcing the benefits of a joint national commitment to tax justice and the promotion of fair competition within the aluminum recycling sector.

Source: Secretaria Especial da Receita Federal do Brasil I (2025).

Box 12. Joint efforts to stop money laundering predicated on tax crime in Indonesia

In 2019, the Directorate General of Taxes established a joint task force to enhance the enforcement of tax crime laws, in particular, the recovery of the proceeds of crime related to money laundering investigations where tax crimes serve as the predicate offense. This collaboration involved several agencies, including the Attorney General's Office, the Ministry of Law and Human Rights, the Indonesian Police, and the Financial Transaction Reports and Analysis Centre (Financial Intelligence Unit). The primary role of the task force is to assist in handling money laundering cases and ensure effective and efficient asset recovery by leveraging the expertise, experience, and data resources of its members. As a result, the number of cases handled increased significantly—by up to 300%—along with a substantial rise in the value of assets seized from money laundering investigations.

Source: Ministry of Finance, Indonesia (2025).

Parallel civil and criminal investigations

Parallel civil and criminal investigations are different from joint investigations in the sense that the different authorities may co-ordinate some investigative activities but carry out separate investigations. This could for example, be a tax audit carried out in parallel to a criminal tax investigation. It is also possible that the parallel matters are not both tax investigations, for example a civil tax audit being carried out in parallel to a criminal investigation into corruption. Such parallel investigations involve a lower level of co-operation between authorities but can still be useful in situations where a joint operation is impractical or undesirable. Depending on the level of co-ordination, authorities involved may share investigative leads, intelligence, and may co-ordinate on operational decisions (e.g., decisions on charging). Generally, both sides conduct their investigations independently, but the advantage of co-ordination is the ability to de-conflict, ensure the fairness and proportionality of outcomes, and take advantage of efficiencies.

Parallel investigations play a particularly key role in jurisdictions that allow authorities to pursue civil tax compliance actions such as audits and criminal tax investigation simultaneously. While civil audits and criminal investigations should always remain separate, authorities may still co-ordinate efforts and share information, while respecting due process. For example, ensuring that civil information gathering powers are not used as a pretext to obtain information for a criminal investigation and vice versa. The TCIM should highlight the importance of defining the scope of co-ordination in parallel investigations, including by addressing any necessary boundaries related to evidence gathering and further use; confidentiality; and/or ethical obligations related to, among others, exculpatory evidence, management and decision-making, or other sensitivities.

Protecting the rights of a suspect when a civil matter becomes criminal

In many instances, criminal tax investigations will start out as an ordinary civil examination or audit procedure. Jurisdictions must therefore have clear laws and procedures in place for what must happen if the situation evolves. For example, in some jurisdictions all civil proceedings must be halted until the criminal investigation is concluded. In other jurisdictions, countries can conduct parallel investigations. The TCIM must clearly define the line that separates a civil tax matter from a criminal tax matter. For example, in many jurisdictions a case would become criminal as soon as there is a reasonable suspicion that a crime has been committed. Other jurisdictions may use an objective marker (such as a threshold for the amount of tax evaded).

Regardless of the approach, the TCIM must clearly state the safeguards that need to be put when there is a change from administrative to criminal law. Failure to do so may not only negatively impact the rights of the suspect, but also have an adverse impact on enforcement, for example, where evidence obtained becomes inadmissible in court because the individual's rights were violated. This is of particular importance in jurisdictions where the tax administration is responsible for both the civil tax (audit) functions and is also mandated to conduct criminal tax investigations.

Box 13. Protecting suspects' rights when a tax audit uncovers criminal activity in New Zealand

New Zealand's (NZ) Inland Revenue's system had flagged that an income tax return filed by Jake, a sole trader painter/decorator, had very high expenses. An investigator (known in NZ as a customer compliance specialist) looked into whether the return was correct. As part of those inquiries, the investigator requested copies of Jake's bank statements and saw a number of deposits that looked like business income, but which had not been included in Jake's income tax return. Jake was asked to attend a voluntary interview. At the start of the interview Jake was cautioned that he could leave at any time, that anything he said could be used in criminal proceedings against him, and that he could have a lawyer present. Jake said he wanted to talk to his lawyer and so the interview ended. The investigator interviewed Jake's accountant who said he had asked Jake to give him all his bank statements and to advise him of any cash payments he had received. The investigator noted that bank statements for the account with the unexplained deposits had not been given to Jake's accountant. The investigator traced the deposits and spoke to the account owners who had paid the money to Jake, who confirmed that the payments were for painting services. The investigator asked Jake to attend another voluntary interview – he refused. Based on the information obtained, the investigator thought this might be an appropriate case for prosecution for tax evasion and the process for deciding whether to prosecute commenced.

In the meantime, the Commissioner of Inland Revenue was able to issue a tax assessment. The assessment triggered a four-month statutory deadline for Jake to dispute the assessment by issuing a notice of proposed assessment (NOPA). A NOPA must set out the facts, law and provide documents to show why the disputant does not agree with the CIR's assessment. This requirement could impinge Jake's fair trial right not to be compelled to disclose his defence prior to a criminal trial. To protect Jake's fair trial rights, the investigator sent a covering letter with the assessment explaining that as prosecution is being contemplated, Jake was not required to provide a NOPA until the question of prosecution had been finally determined (this would either be the CIR deciding not to prosecute or the conclusion of the criminal process). This approach is permitted under NZ's legislation which allows the CIR to accept a NOPA outside the statutory timeframe in exceptional circumstances. Protecting a taxpayer's fair trial rights constitutes an exceptional circumstance. The letter also explained that Jake could choose to issue a NOPA on a voluntary basis and warned that this could be used in any criminal proceedings. The investigator recommended that Jake seek legal advice before providing a NOPA at this stage. Jake wanted to dispute the tax assessment but chose not to issue a NOPA, reserving his position for a criminal trial. The prosecution progressed and the criminal court found Jake guilty of tax evasion. After the prosecution the investigator wrote to Jake to resume the civil tax dispute. Jake continued to dispute the tax assessment but ultimately this was upheld by the civil court.

Source: Inland Revenue, New Zealand (2025).

Box 14. Use of parallel civil and criminal tax investigations to deter abusive tax schemes in the United States

Pursuant to section 9.5.3.2.1.4(3) (https://www.irs.gov/irm/part9/irm_09-005-003%22%20/l%20%22idm140307901075808) of the IRS Internal Revenue Manuals, regarding Criminal Investigation Strategies, abusive tax schemes investigations often utilise parallel proceedings to effectively halt such schemes and safeguard Treasury revenue. These parallel proceedings are clearly distinct and separate civil and criminal investigations, and do not entail joint efforts. Particularly, IRS Criminal Investigation, the Small Business/Self Employed (SB/SE), and Department of Justice (DOJ) have developed co-ordinated strategies to apply both civil and criminal statutes in co-ordination for parallel investigations. The advantages of using parallel proceedings against promoters of abusive tax schemes include:

a. An injunction typically halts the promotion much earlier than criminal enforcement alone.

b. Filing an injunction, along with a press release, swiftly communicates the government's stance on a promoter or scheme.

c. Parallel investigations allow civil and criminal agents and government attorneys to share information where appropriate, enhancing the efficient use of government resources."

Source: US 2020, IRS Internal Revenue Manuals, 9.5.3. Criminal Investigation Strategies, Section 9.5.3.2.1.4, Abusive Tax Schemes.

Secondments and co-location of staff

Secondments and co-location of staff between tax and financial crime authorities are an effective way of promoting skills transfer while allowing staff to build knowledge and relationships within agencies with a shared goal of fighting illicit financial flows. Jurisdictions utilising these arrangements report wide-ranging benefits including enhanced detection, better intelligence sharing, more proactive cross-agency engagement and more streamlined collaboration resulting in improved case outcomes. The TCIM should identify any underlying legal or operational frameworks in place that facilitate such arrangements and encourage staff to identify instances where they would be of mutual benefit (for example, where agencies are facing common threats, investigating the same suspect or criminal networks, where an agency requires support on a particular area of expertise held by another agency, etc.).

13 Government databases and registers available to tax investigators

Beyond the information held by other government financial crime authorities, civil and criminal tax investigators may have access to a range of other government registers/databases. A TCIM should both raise awareness of these as potential sources of intelligence, evidence, and as tools for tracing assets. The TCIM should provide guidance on when and how they can be accessed by law enforcement. Examples include government registers of:

- Citizens and residents;
- Basic and beneficial ownership information pertaining to legal entities and/or arrangements (other than trusts/fiduciary arrangements) for example, public limited/traded companies, limited liability companies, general partnerships, limited partnerships, non-profit organisations, foundations, associations, etc.;
- Trusts and other similar fiduciary arrangements;
- Bank accounts;
- Financial assets (e.g. cash or cash equivalents, bonds, fixed deposits, equity shares, mutual funds, exchange traded funds, insurance contracts, derivatives, employment benefit schemes, etc.);
- Border movements and customs declarations;
- Land and real-estate;
- Motor vehicles, vessels, aircrafts;
- High value goods/assets (e.g. artworks, precious metals and stones, etc.);
- Social beneficiaries;
- Politically Exposed Persons (PEPs); and
- Lists of persons and entities subject to targeted financials sanctions under UN and/or domestic regimes (e.g., AML/CFT/CPF).

To promote transparency and access to these registers, the manual should also identify:

- Whether the registers are centralised or decentralised (i.e. between different states, regions, etc.)
- The name(s) of the agency or agencies that hold/maintain the register;
- The contents of the registers
- The extent to which tax authorities and tax crime investigators have access to these domestic registers (e.g. publicly available, direct access, access on request, restricted access, access with court order only, etc.)
- The format and searchability of the registers (digital or otherwise).

Because beneficial ownership (BO) information pertaining to legal persons can be of relevance to uncover the natural persons who own, control, or benefit from assets, this category of information and the options available for obtaining it may warrant a dedicated discussion in the manual. Jurisdictions will use a multi-pronged approach that allows tax and other authorities conducting investigations to obtain or access BO information, including by (i) requiring the company itself to obtain and hold this; (ii) maintaining it via one or more public authority or body (e.g., in a register); or (iii) using an alternative mechanism (e.g., collection and verification by financial institutions). Adequate, accurate, and up-to-date BO information should be available to tax investigators in a timely fashion, for both companies created in the jurisdiction and foreign companies having sufficient links with the jurisdiction, as well as on trusts and other similar legal arrangements (see Recommendations 24 and 25 on transparency and beneficial ownership of legal persons and arrangements, respectively (FATF, 2012-2025[7]).

Box 15. Project to map jurisdictions' access to centralised government registers accessible to tax authorities and tax crime investigators

In 2023, the OECD launched a project to map jurisdictions' maintenance of different types of centralised domestic government registers to better understand their contents and the extent to which they can be accessed by both civil and criminal tax investigators. Over 50 jurisdictions have already completed this comprehensive survey which is a valuable source of information for agencies domestically and also an important tool for the purposes of cross-country mapping. If your jurisdiction is interested in completing this survey or gaining access to a survey previously completed, please contact the secretariat at OECD.TaxandCrime@oecd.org.

14 The role of whistleblowers in tax crime investigations

A whistleblower is an individual who reports misconduct, illegal activity, or other wrongdoing within a private sector organisation or government entity, including within tax authorities and law enforcement agencies. Whistleblowers can play a key role in uncovering tax other financial crimes that would otherwise be difficult to detect and enhance the success of a prosecution. The TCIM should provide detailed information on the jurisdiction's tax whistleblower framework, including:

- **Internal reporting channels:** Typically managed by an internal integrity unit, the tax crime investigation agency should have established channels in place for confidential reporting by internal whistleblowers (e.g. through dedicated hotlines or secure web portals);
- **External reporting channels:** There should be clear and publicly accessible mechanisms in place for individuals from other public sector agencies and private sector organisations to report suspected criminal tax activity to the tax crime investigation authority;
- **Confidentiality safeguards:** To encourage reporting, jurisdictions should have laws and procedures in place to protect the whistleblower's identity;
- **Protections from retaliation:** Jurisdictions should have comprehensive safeguards in place to protect whistleblowers from reprisals for protect disclosures, including protections from termination of employment, lawsuits, and/or criminal prosecution;
- **Legal and financial support:** Many jurisdictions have provisions in place to provide legal and financial support to whistleblowers who may have experienced reprisals;
- **Incentives:** Some jurisdictions have formal tax whistleblower programmes in place offering rewards such as financial incentives where taxes are recovered as a result of the report.

Box 16. Tax whistleblower programmes in Liberia and Korea

Liberia Revenue Authority launches online whistleblower platform

In February 2025, the Liberia Revenue Authority (LRA) launched its online whistleblower platform to strengthen the fight against tax evasion and enhance the integrity of revenue collection. The platform, accessible via the agency's website, is designed to encourage citizens and the general public to report tax evasion, fraud, and related financial crimes, including malpractices and corrupt activities by both LRA and non-LRA staff. Whistleblowers will remain anonymous and protected unless they choose to disclose their identity. Through the platform, individuals from both the public and private sectors can report suspected cases of tax evasion involving businesses and individuals. The LRA will provide a taxable proportional award of 5% of the net taxes or duties recovered from tax fraud or evasion, in accordance with Section 16 of the Liberia Whistleblower Act of 2021. Additionally, LRA is developing and delivering educational programmes to inform the public on how to use the platform effectively."

Source: Liberia Revenue Authority (2025), https://eservices.lra.gov.lr/lraWhistleBlower/blow_wh_nologon

Rewarding tax whistleblowers in Korea

In Korea, under the National Tax Service's (NTS) Tax Evasion Informant Reward Program, an individual with "significant information" on tax law violations can disclose their evidence to the NTS. If proven true, they may qualify for a monetary reward between 5% and 20% of the proceeds collected by the NTS as a result of the informant's disclosure, provided the amount exceeds KRW 50 million (approximately USD 35,500). In addition, through the Foreign Financial Account Report Reward Program, foreign accounts are also covered, with a maximum reward of 15%. The program allows potential whistleblowers to disclose information on foreign financial account violations

Source: National Tax Service, Korea (2025)

15 Power to search property and seize physical and digital evidence

Investigations into tax crimes and other related offences may necessitate the investigation team to lawfully enter a property, either with or without prior notice and search for, and seize, any physical and digital evidence that may be relevant to the ongoing case. Such search and seizure operations may also used by law enforcement to restrain the suspected proceeds of crime to ensure offenders do not profit from their illicit gains.

These investigative steps may involve the seizure of cash, devices, or other objects for the purpose of evidence and/or potentially for their value for asset recovery purposes. The manual should distinguish between these purposes (even if the same item may be relevant for both) as well as distinguishing between provisional measures to preserve criminal property for potential confiscation, and the unplanned seizures of property which may result from opportunities such as searches conducted on premises (see section 17 on asset recovery for more detail).[3]

In some instances, particularly where an investigation is becoming overt or is at its resolution stage, search and seizure operations may be combined with the arrest and interview of any suspects present at the search location. Accordingly, conducting lawful searches of premises requires significant planning and co-ordination of resources to optimise their success

As with all stages of an investigation, the processes in place for the search and seizure of digital and physical evidence will vary from country to country. To that end, the following sections provide a high-level guide on the different factors for investigators to consider at each stage of a search and seizure.

Physical versus digital evidence

In tax and other financial crime investigations, commonly seized physical items include books, records, cash, and any other physical materials that may be evidence of a tax crime. Any physical evidence obtained by law enforcement through search and seizure measures must be subject to stringent chain of custody requirements to ensure evidence is not contaminated or tampered with and can later be used as evidence in court. To be effective, jurisdictions must have dedicated processes in instances where large amounts of

[3] Criminal property which should legally be subject to confiscation and provisional measures (e.g., temporary restraint or seizure to preserve assets for potential final confiscation) includes (1) the proceeds of offences; (2), the instrumentalities used in or intended for use in offences; and (3) property laundered, among other categories. For additional information on the essential components of a jurisdiction's asset recovery framework, please refer to the FATF Recommendations (www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html, Recommendation 4 (Feb. 2025 ed.) (on confiscation and provisional measures).

cash, or unlawful physical items such as illicit drugs or illegal weapons are identified during the search exercise.

By contrast, digital items refer to electronic devices such as computer hardware, software, tablets, cell phones and other electronic media, including cloud storage that may contain important digital evidence (e.g. emails, text messages, electronic documents, banking records etc.)

As noted under Principle 4 of the Ten Global Principles Guide: “during a physical search of a home or office, documents can be reviewed in a manner that quickly indicates whether or not they are covered by the search warrant and relevant to the investigation. However, digital media may contain hundreds of thousands of e-mails, documents and text messages, created over many years, and not necessarily related to the tax crime. It is therefore challenging, if not impossible, to determine during the onsite search whether or not a particular piece of electronic information is covered by the search warrant and its relevance. Therefore, the search may include digitally copying or imaging the data that is held, and examining the contents in a digital forensic lab in order to determine which pieces of the information are within the scope of the search warrant and relevant to the case under investigation.” (OECD, 2021[6])

There may also be legal challenges connected with the search and seizure of digital data in computers and other electronic devices. Personal data in an electronic device may not be relevant to the suspected tax crime, or may contain data protected by a legal professional privilege. This may require that the search is carefully governed to ensure it is limited to the terms of the authorisation. There may also be legal challenges connected with the search and seizure of computers and other electronic devices. This may be particularly pertinent in cases where the search powers contained in the law refer explicitly to searches or seizure of physical documents, or where a person challenges a search of digital media on the basis that it is overly broad and goes beyond the terms of the search authority or could include privileged documents”. (OECD, 2021[6]).

Box 17. Seizing digital evidence in Australia

In Australia, police have the power to operate electronic equipment found at a search warrant premises to access data (including data not held on the premises). If the data accessed is evidential material, it can be copied and removed by operating the equipment or, if it is not practicable to do so, seizing the equipment. A computer or data storage device, including a mobile phone, found at the warrant premises may be removed for up to 30 days if police believe on reasonable grounds that the device contains evidential material. Additionally, if the device suggests the existence of a digital asset that may be seized under a warrant, it can be taken for examination or processing in order to determine if it may be seized under the warrant. This is permissible if it significantly more practicable, considering the timeliness, cost of examining or processing the item, and the availability of expert advice. The occupier or someone representing them must be notified of the time and place that the examination is to take place, and officers must allow the person or their representative to attend the examination unless it is not practicable to do so. This has proven particularly useful in large complex tax and fraud investigations, in which large amounts of data must be searched on the digital media in order to identify the relevant evidence.

Source: Australian Federal Police (2021)

Pre-search considerations

Conducting property searches requires significant planning and co-ordination, particularly when carried out simultaneously across several locations. Before considering a search, investigators should weigh up the anticipated benefits and requirements including:

- What locations are to be searched and what is the significance of these sites to the investigation?
- What information or items (digital or physical) are believed to be present at the search location(s)?
- How certain is it that the desired evidence exists and will be at this location?
- What intelligence or other information substantiates this?
- Can the target information and evidence be obtained through alternative means?
- Will any of this information or evidence be subject to any legal professional privilege?
- Will conducting the search at this stage of the investigation have any negative impacts?
- Who, if anyone, is likely to be present at the premises (suspects, subjects, or third parties)?
- Will the search operation coincide with any arrests of suspects or seizure of suspected criminal proceeds?
- Is there a possibility of resistance to the search, obstruction, or the destruction of evidence?

Depending on the jurisdiction, it could be beneficial to include these and other similar considerations in a template or checklist for investigators to complete for recordkeeping and review purposes. This can help justify the decision-making process in case of any external scrutiny of use search and seizure measures. As with all documentary requirements included in the TCIM, it should be accompanied with an explanation for staff on how to access, complete, and store this information.

Obtaining approvals and warrants

The TCIM should outline the underlying legal basis that empowers investigators to conduct searches of property. Understanding the applicable legislation is important for several reasons. First, an officer must understand both the scope and limitations of the power as well as the rights and obligations applicable to the target. This will ensure the investigator can provide appropriate explanations and reassurance to any persons present during the execution of the search warrant. Having this understanding will ensure the investigator is aware of the requirements for both internal and external approvals (e.g. a court warrant). At a minimum, the TCIM should:

- Clearly explain any internal and external approval processes for search and seizure operations;
- Provide hyperlinks or instructions on where to obtain any necessary approval forms, templates or documentation, etc. (for example for obtaining the warrant itself, letters formally requesting assistance from other agencies required to execute the search, etc.);
- Include detailed instructions on how to complete any forms (noting that many elements of a search warrant application will be the same as those outlined in the search plan itself, as laid down in the subsection below);
- Include the contact details of officers from whom advice or assistance can be obtained where necessary;
- Include instructions of where to submit documents for approval and how to store these submission requests, supporting documents, and any subsequent approval/rejections in the case management tool or file.

Formulating a search plan

Once approval to conduct a search is obtained, investigators will need to plan the logistics of the search operation. A well-executed plan enhances the efficiency of the operation, increasing the likelihood of the investigation team securing the required evidence. Executing a successful search requires comprehensive planning and extensive co-ordination of resources, often across different agencies. Furthermore, it is imperative that contingencies which may arise are anticipated, mitigated against, or otherwise planned for. Accordingly, a TCIM should provide guidance for investigators in formulating a search plan that details the intended actions to be undertaken and acts as a resource for all internal and external stakeholders involved. Table 3 includes a non-prescriptive, non-exhaustive, list of topics that are commonly included in a search plan.

Table 3. Common elements to include in a search plan

Contents	Description
Lead investigator	Contact details of the lead investigator who can be contacted for any questions stakeholders have during the search pertaining to the case itself and the potential relevance of any evidence that may be discovered.
Resources and budget	Required agencies, team members, travel budget, anticipated man hours.
Required documentation/approvals	Prior to the search operation, it necessary to assign an officer in charge of ensuring all of the required documentation is in place (e.g. search warrant approved and signed, search approval, letters of request to other agencies sent, etc.)
Case background	A brief summary of the case that provides context to officers, including the basis for the case being initiated, initial findings to-date, known facts, and any current suspicions. This could include flowcharts of any known or suspected behaviours or criminal methods to help stakeholders understand the case context.
Purpose of search and key physical and digital items sought	The reasons for the search including any potential physical or digital evidence being targeted. The importance of this section in the search plan cannot be overstated, as the primary goal for the search team members is to secure the specified evidence. This should include available information pertaining to computer systems, as well as other information technology-related equipment that may be present on the premises being searched. In light of the possibility that suspects may own virtual assets, instructions on how to identify wallets, keys, seeds, or other indications of virtual asset holdings, plus how these can be secured into government custody effectively (if they are sought for seizure). It is vital for the search team to possess a comprehensive understanding of the documents that need to be located and seized during the search operation.
Taxpayer(s) information	Basic information about all suspects under investigation including known associates and related parties. Including this information across all search plans assists officers engaged in the search to ascertain between relevant and irrelevant information and evidence they will uncover during the search. Including visual aids such as charts that show the suspects, their related entities, authorised representatives and their respective relationships to one another, can assist stakeholders understand the case context.
Stationary and storage items	Checklist of stationary items required and person in charge of packing these (e.g. evidence bags, gloves, masks, cutters, extension cables, envelopes, scissors, staplers, pens, etc.).
Electronic equipment/devices	Checklist of all electronic equipment/devices for carrying out various tasks during the search operation and assigning an officer to check their functionality prior to the search. (e.g. ensuring camcorder, camera, and voice recorder memory cards are formatted, fully charged, and have sufficient storage capacity to store videos, photos and recordings, including backup storage mediums).
Command centre details	Contact details of the focal points in any command centre where all milestones and key developments can be communicated and recorded (see below section on command centres for more information)
Auxiliary staff	Contact details of staff that are assigned to act as go-betweens between the headquarters and sites to respond to any requests for assistance or provide additional materials to investigators on location, as required.
Safety/risk assessments	Where any of the suspects that will be subject to a search are identified as potentially posing a safety risk to investigators, this should be communicated to all stakeholders and appropriate counter measures taken, such as engaging Police or Special Weapons Units to secure a location before search staff enter the property. Some common indicators include (a) any prior interactions of concern with law enforcement or any other relevant intelligence; (b) any known history of violence or aggressive behaviour; and (c) any inclusion on databases that indicate association with criminal gangs or terrorist groups, as well as possession of legal or illegal firearms.

Site leader	A senior officer should be nominated as a site leader at each location and their contact details noted.
Meeting point	A location in close proximity to the target location for stakeholders to gather prior to executing the search. The location selected should mitigate against potentially alerting the target of an impending search operation particularly in searches being conducted without notice.
Site location	The address of the property to be searched, including any noteworthy characteristics of the site. Photographs of the location as well as directions from the pre-search meeting point can also be included to aid staff.
Site purpose	The reasons for searching this location and key objectives (taking care to not narrow the objectives).
General operational information	Date and time of search.
Anticipated persons present	Details of the persons who are expected to be encountered on-site.
Emergency assembly point	In the event of an emergency occurring during the search, all stakeholders should be aware of a pre-selected emergency assembly point to rendezvous.
Search contingencies	Depending on the jurisdiction, it may be relevant to include details such as contact details for the nearest police station or a locksmith. It may also be prudent to advise local law enforcement in advance that the tax crime investigation agency intends to execute a search.
Search execution plan	An agenda of the anticipated tasks to be undertaken, the officers assigned to the specific tasks, as well as the projected duration of each action. This allows all members of the site-team to have an understanding of their respective roles and responsibilities during the search.
Appendices	Attach all applicable appendices that substantiates the facts and findings written in the search plan

Pre-search orientation meeting

Once the search plan is formulated and a search team assembled, the TCIM should provide processes for conducting a pre-search orientation meeting to be convened between all stakeholders participating in the search operation. A pre-search orientation meeting provides the investigation team with an opportunity to:

- Brief all stakeholders about the search activity and for questions to be asked and answered;
- Orient staff with their respective search teams and site leaders;
- Distribute and discuss search plans;
- Remind stakeholders of any secrecy or confidentiality requirements pertaining to the search, where applicable, as well as any relevant procedures for dealing with any press/journalists, associates, supporters and bystanders who may arrive during the operation;
- Ensure all relevant equipment within search kits are adequately stocked and distributed to site leaders as well as necessary equipment such as investigator's badges or signed authorities.

Site identification and surveillance measures

Conducting searches of property may, depending on how the investigation is being conducted, be the first moment a suspect is made aware that they are under investigation. In these instances, it is imperative to identify all potential sites that should be subject to a search to mitigate against any potential destruction of evidence.

Additionally, it is critical that the location of the suspect is known at the time a search plan is executed. For example, if a search of the suspect's dwelling is conducted after a suspect has left the property and their exact whereabouts are unknown, there is a chance that any evidence in their immediate possession such as mobile phones, laptops, or other documents could be destroyed if they are notified that their dwelling has been subject to a search operation by law enforcement. To this end, an investigation manual should also include advice for investigators to consider utilising tracking powers and surveillance of the suspect and their relevant associates, as is appropriate and allowed under law. Additionally, a manual should also consider including processes that investigators can refer to if they need to apprehend a suspect beyond the search location and conduct a search of their person to secure any critical evidence.

Locations such as the suspect's dwelling, workplace, or those of their respective associates and advisors are commonly identified as potential targets, but employing surveillance powers can also identify additional sites for consideration, including for identifying where assets that may be relevant for seizure action, could be located. An effective manual should therefore provide guidance on identifying the potential sites to consider subjecting to a search as well as the tools and approaches available to determining any additional sites.

Command centre

As noted above, search procedures in criminal matters are often conducted simultaneously over several geographic locations, necessitating a central communication hub that can monitor, manage, and co-ordinate the various search operations in real-time. The command centre serves as focal point for site leaders across all search sites to communicate developments as they occur and for decision makers to communicate directions, advice, and solutions back out to the field. Where an unexpected development arises in one location, this can be contained between the site and the command centre while it is addressed, allowing the other sites to continue with their respective search roles. Command centres can also co-ordinate the efficient allocation of resources, for example where one location requires less manpower than anticipated, these additional excess searchers can be directed by the command centre to an alternative location requiring assistance. The command centre also plays a role of logging and recording events across all of the sites as they occur for transparency, accountability and evidentiary purposes.

Some jurisdictions may have dedicated rooms for this purpose within their headquarters and in others this will need to be established by investigators in a conference or meeting room. Command centres need to be specially equipped, both by staff and with the necessary tools including dedicated phone lines, materials to log events in real-time as well as the resources to display live statuses and timelines for each site. In either case, an TCIM should advise investigators on the purpose of, and how to operate the command centre during search operations. Similarly, search officers in the field should also be aware of the role of the command centre and the events and other required reporting they need to communicate into the command centre.

Executing the search

Search procedures and the seizure of evidence and criminal proceeds are governed by legislation and other regulations requiring strict adherence by staff to ensure they are conducted lawfully. There are often separate and unique procedures to follow when documenting and removing different classes of evidence such as those for physical cash and digital hardware.

The below table includes a non-exhaustive list of different steps in the search that a TCIM should provide guidance on. For every step, the manual should include the:

- Legislative provision underpinning the action;
- The operational process to follow, including the person(s) responsible and required documentation;
- Links to any other relevant resources to ensure the smooth execution of the search.

This is critical for ensuring that the searches are conducted legally, thoroughly, and to preserve the integrity of the evidence for later use in court.

In most jurisdictions, searching certain premises such as a lawyer's office, and seizing documents under legal professional privilege, should be performed following specific legal provisions. The TCIM should also address this matter where appropriate in order to provide officials with the necessary guidance to successfully conduct such search.

Table 4. Common elements of search execution

Action/Instruction	Purpose
Pre-entry	
Assembly of all site search team components and recording their attendance.	Provide officers with precise instructions on where and when to meet.
Approaching the location	Instructions to prevent altering the suspect to an impending search (e.g. avoid lingering at the entrance).
Entering and securing a search location	
Serving of warrants.	Ensures officers are clear on when, how, and to whom to serve the warrant upon entering the premises.
Gaining access to the property.	Avoids delays.
Securing the property and containing potential threats including making arrests.	Promotes a safe search.
Advising suspects of their rights and the powers being exercised by law enforcement.	Ensures suspects' rights are protected and evidence is preserved (see section 24)
Note taking/search log	
Handling of evidence	All officers must be aware of the process to follow upon handling evidence e.g. items seized should be sealed immediately in an evidence bag, issued a number, and chain of custody document attached (see below).
Photography and videography of the search.	Photography and videography provide visual evidence of the search operation, capturing the condition of the premises, the location of items, and any relevant details. These records serve as an official account of the operation and can be used for future reference or legal proceedings as well as for staff training.
Chain of custody documents for different types pf evidence seized (digital media, physical cash, paper documents)	To preserve the integrity of evidence, it must be recorded in a manner that can be used for authentication and attribution through a clear chain of custody. The chain of custody is the record (paper and/or digital) showing the collection, custody, control, transfer, analysis, of evidence. It plays an essential role in ensuring the integrity and admissibility of the evidence in legal proceedings. All documents should include the date and time of seizure, description of evidence, seizing officer's information, and the exact location where the evidence was seized or found.
Inventory list	Inventory lists contain the details of confiscated items during the search operation. It serves as a formal notice to the taxpayer that the search team has seized custody of the item(s) and that they may be used as admissible evidence. It is recommended that jurisdictions develop a template for this and annex it to the TCIM.
Comprehensive records of all persons present (e.g. including personal information, job title, etc.	To facilitate summons interviews with employees and other witnesses at later interviews and facilitate connections between employees, as well as other relevant information.
Exiting the search location	
Clearing the location	Instructions to pack all documents and equipment brought by the search team so that nothing is left behind and to inform key parties that the search is complete.
Post-search works	
Instructions on depositing seized items to evidence room	To secure chain of custody, seized items must be promptly placed in a secure evidence room, logged in a registry that includes the specific details on the item as well as the date, time, and the officer responsible for depositing the item to the evidence room.
Search warrant execution report	A full report should be prepared and disseminated as appropriate.
Download of digital evidence and return of seized items	Instructions on how to return seized items once its purpose has been fulfilled.
Forensic analysis	Instructions on how seized items (physical or digital) should be submitted for forensic analysis, ensuring that the chain of custody is preserved.

16 Evidence management

Once digital and physical evidence related to an investigation is obtained, it is critical that it is handled, documented, and preserved in a systematic manner to integrity and admissibility throughout the criminal justice process, including ensuring that all available evidence is disclosed to the accused in accordance with criminal procedure laws.

Physical evidence

Physical evidence seized during a search are stored in a secure location, designated by the legal framework of each jurisdiction (ordinarily in an Evidence Act, Criminal Procedure Code or both. This space (often referred to as an 'evidence room' must be restricted to authorised personnel only and the depositing of, and access to this evidence must be strictly regulated through use of a register.

The TCIM should raise awareness among officers of the importance of evidence management and outline:

- Who within the unit is responsible for placing evidence in the room (ordinarily in designated lockers);
- Who is responsible for completing the evidence register;
- Who can access the room and for what purpose. For example,
  - The room may be made available to the prosecutor's office upon written request for the purposes of disclosure to the defence and presentation of evidence in court;
  - Evidence may also be accessible by other officers who need to retrieve the evidence for case related work (e.g. forensic analysis).
- The types of information that should be recorded in a register whenever evidence is removed. For example,
  - The name and details of the person who retrieved the items from storage
  - Details of the items taken
  - Purpose of removal
- Date and time items were removed.
- Date and time items were returned

Digital evidence

In the case of digital media, it is essential that tax and law enforcement authorities have access to digital forensic tools that enable them to identify, acquire, extract, preserve, document, analyse, and present digital evidence in a methodical, proficient, and repeatable manner. These tools will typically be housed within a dedicated digital forensic laboratory (DFL).

Similar to physical items held in an evidence room, the TCIM should outline in detail the standard operating procedures for handling of digital evidence to ensure that criminal cases do not fail on account of corruption, contamination, destruction, tampering, or any other improper handling of the digital evidence over the course of the investigation. Basic procedures for the handling of digital evidence is outlined below. For more detailed information on the handling of digital evidence, please refer to Interpol's Global Guidelines for Digital Forensic Laboratories (INTERPOL, 2019[15]).

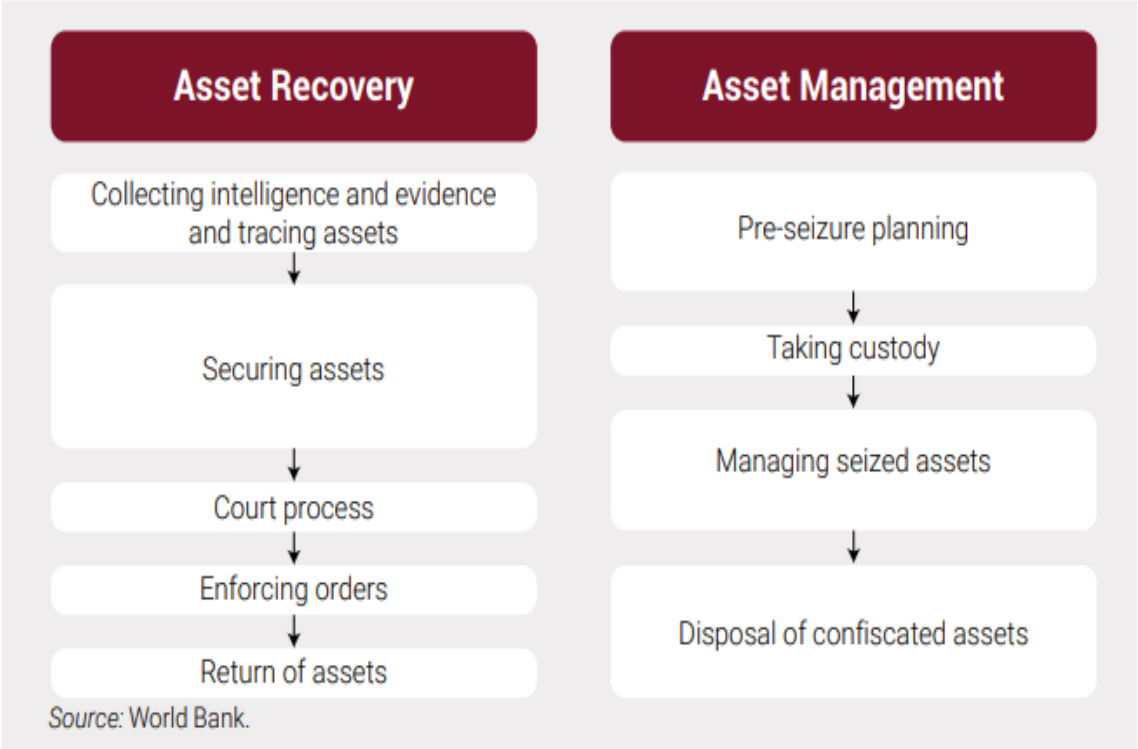
Table 5. Management of a digital forensic case

Stage of case	Description
Receive request	Once an electronic item has been seized, the investigating officer will typically send a formal request to the DFL, including a description of the criminal act(s), details of the electronic evidence, and objective of the case. The lab manager will then assess whether the case is feasible based on its scope, available tools, available staffing, and whether the legal requirements are fulfilled,
Register case	If accepted, the officer will bring the electronic device to the DFL and complete a case registration form with a clear and specific case request so that the lab examiner can determine the appropriate methods and tools to employ. Both parties should sign the form, and a dedicated case file will be created.
Register exhibit	As with physical evidence, digital evidence must be subject to stringent chain of custody procedures. Each piece of electronic evidence must be registered and assigned a unique identifier which is documented with the exhibit's details in the registration form. This includes sub-items such as sim cards and memory cards. Any defects must be document to protect against future claims of damage. While the exhibit is not in use, it must be stored in an evidence room (following the procedures described in the subsection on physical evidence above).
Photo exhibit	A photograph of each item should be taken as a record of its state and to enable it to be identified in the future. The photo should then be uploaded to the case file.
Conduct analysis	Analysis of digital evidence must be conducted in accordance with the DFL's standard procedures. Throughout the analysis stage, the examiners should remain in contact with the investigating officer to communicate any limitations or other issues that may arise. Clear communication is the most effective way to ensure that the correct data is identified.
Return exhibit	Once the analysis is complete, the lab examiner should contact the investigating officer to collect the evidence. Typically, all electronic items are returned together with the forensic report in a sealed bag containing the exhibits label, date and time sealed, and staff's signature.
Close Case	To close the case, both the requesting officer and the examiner must agree (and sign) that the report has been delivered and the work is complete. The requesting officer will notify the examiner if/when they are needed in court to provide expert testimony on the forensic analysis.

17 Asset recovery

Asset recovery refers to the process of identifying, seizing, confiscating, and returning assets that have been obtained unlawfully, for example, through the commission of a tax crime, corruption, or money laundering. Its purpose is to strip criminals of both the instruments and proceeds of crime and to return such property to its legitimate owners or to compensate victims. To achieve effective asset recovery, jurisdictions must also have in place effective asset management systems designed to preserve the value of seized assets and maximize the value of the disposal of forfeited assets. Asset recovery may be conducted through a variety of legal avenues, including through both civil and/or administrative processes and/or criminal proceedings, and may be called confiscation or forfeiture depending on the jurisdiction. However, regardless of the legal avenue, the fundamental process for the recovery and management of assets remains the same (Bostwick et al., 2023[16])(FATF Recommendations, General Glossary definition of “asset recovery” (FATF, 2012-2025[7])).

Figure 8. Processes for asset recovery and asset management



Source: World Bank (2023)

Asset recovery plays a central role in any tax crime investigation and the TCIM should outline in detail the applicable legal and operational processes that must be followed by investigators to effectively identify, restrain, preserve, and ultimately recover assets linked to a tax crime. For more detailed guidance and international best practice with respect to asset recovery, see the list of global resources included in Box 20 at the end of the section.

Asset freezing and seizing

The freezing or seizing of assets involves "temporarily prohibiting the transfer, conversion, disposition, or movement of assets or temporarily assuming custody or control of assets on the basis of an order issued by a court or other competent authority" (UNODC, 2004[17]). Freezing is a provisional action that temporarily suspends the owner's rights and control over the asset, and usually leaves them under the administration of a third party (e.g. for bank accounts). Seizure, by contrast, is an action to temporarily take possession of an asset or put it into the custody of the government (e.g., for physical assets such as a vehicle) (see also FATF Recommendations General Glossary definitions of '"freeze and seize" (FATF, 2012-2025[7]). Generally, these measures are used to temporarily prevent the movement of assets pending the outcome of a case and are vital for preventing the dissipation of assets, disrupting ongoing criminal activity, and preventing victims from further harm. Moreover, the capacity to freeze and seize assets ensures that funds remain available for future confiscation/forfeiture (see section below); asset recovery measures; the payment of fines or penalties; and/or victim compensation.

Criminal property which should be legally subject to freezing and seizing (and later confiscation) includes the proceeds of crimes, instrumentalities used in or intended for use in crimes, and property laundered.[4] There are also less invasive, temporary measures whereby jurisdictions should be able to suspend or withhold consent to transactions suspected of being related to money laundering or predicate offences (including tax crimes). This latter power is of a limited duration (often a matter of days) and may be wielded by the jurisdiction's FIU or another competent authority. It may be helpful as stop-gap measure, to allow the FIU or law enforcement to analyse and confirm suspicious activity and enable tax investigators to gather sufficient evidence to obtain a more lasting provisional measure (see also the Interpretative Note to Recommendation 4 (FATF, 2012-2025[7]).

This part of the TCIM should clearly identify when and how freezing and seizing powers can and should be used and the processes for doing so (including links to applicable templates/checklists for the required applications).

Procedures for asset freezing and seizing

The procedures in place for the freezing and seizing of assets vary between jurisdictions. While in most jurisdictions, these can only be carried out upon obtaining an order from a court or a prosecutor, in other jurisdictions, agencies may hold this power directly (e.g. upon approval of a Commissioner).

The TCIM should describe in detail the processes that officers must follow to utilise asset freezing and seizing, including whether these can and should be applied on an *ex parte* basis (i.e. without prior notice to the affected person).

Speed is also an important consideration when it comes to provisional measures, as criminals can quickly transfer funds outside of agencies' reach or dispose of property if they become aware that they are under

[4] For additional information on the essential components of a jurisdiction's asset recovery framework, please refer to the FATF Recommendations, Recommendation 4 (Feb. 2025 ed.) (on confiscation and provisional measures).

investigation. Depending on the jurisdiction, authorities may have legal powers to execute rapid freezing orders (e.g. within 24 and 48 hours) where loss of property is imminent.

Finally, jurisdictions should ensure that they have the capacity to execute freezing and seizing orders pursuant to domestic cases and on behalf of foreign jurisdictions, who may request an order pursuant to a bilateral or multilateral treaty (see section 20 on international co-operation).

Regardless of the process, the TCIM should provide detailed instructions, reference the underlying legislative provisions, and provide links to the documents and templates for such applications to ensure all relevant officers are aware of and have access to these tools.

Common elements included in asset freezing and seizing applications may include:

- Details of the person who is the subject of the order or warrant;
- Details of the suspected crime committed, being committed or about to be committed;
- Detailed description of each asset to be frozen or seized (e.g. cash, real-estate, vehicles, bank accounts, securities, virtual assets, etc.);
- Some evidence of the crime committed, being committed or about to be committed (i.e., enough to meet the legal threshold for the tool to be applied, such as reasonable suspicion, probable cause);
- Explanation of the connection between the assets and the alleged crime (including whether the assets are the proceeds of crime, instrumentalities used to commit the crime, or laundered);
- Legal citations to specific offences and laws authorising the provisional measure;
- Date and time periods for which the assets should be frozen or seized;
- Identification of any third-party interest or claims to the assets;
- Estimate of the asset's net value including any encumbrances (for example, a mortgage);
- Evidence that the subject of the order has been notified (or justification for applying the order on an ex parte basis); and
- Instructions on with agency/authority should seize the asset or which third-party should administer it, depending on whether the order is a freezing or seizing measure.

Box 18. Asset freezing and seizing in Belgium

The CTIF-CFI is an independent administrative authority with legal personality. It has the authority to freeze all transactions on bank accounts according to Article 80 of the Anti-Money Laundering Law of 18 September 2017 when they notice suspicious activity. The CTIF-CFI will make a report following such freezing and inform the public prosecutor's office. The public prosecutor can then seize the assets on the bank account and place them under the care of the COIV, which is also a separate part of the public prosecutor's office. The seized money can later be used to pay criminal fines imposed by the judge, as well as taxes and other penalties.

Since July 17, 2017, investigators within Belgium's STI can use Article 52*bis* of the VAT Code to seize movable property that doesn't exclusively belong to other parties if, following the investigation, they determine a set of consistent indications of serious fraud exist, whether organized or not, and have contributed to the violation of VAT legislation. While the property is not physically seized, the measure entails a limitation on it being sold for up to 3 years. Violating the imposed limitation is a criminal offence for the seller of the seized movable property

The article has a very strict framework form with deadlines and has a built-in judicial oversight of the seizure. The law was put to test in 2018 during an investigation of a furniture company, when investigators discovered that the company issued delivery receipts to customers but did not have invoices for these deliveries. According to preliminary calculations, the VAT fraud amounted to €134,217.77. The investigators also noticed that the company was advertising a stock sale of their showroom models with high discounts, raising concerns that the company intended to make itself insolvent. Based on Article 52bis, the investigators searched the business premises and seized two cars and all showroom models in the furniture store. The final taxation, with definitive numbers, amounted to €299,516.87 in VAT (excluding fines). The seizure was confirmed by a judge.

Source: FPS Finance, Belgium (2025).

Asset management

As outlined at the start of the section, effective recovery of asset relies heavily on jurisdictions having effective procedures in place for the management of frozen or seized property to preserve its value pending a final court decision. As such, the TCIM should identify the jurisdiction's mechanisms or agency for managing, preserving, and, when necessary, disposing of frozen or seized property. Typically, this will be a dedicated asset management office or a judicial entity with a similar mandate, which is specialised in safeguarding the value of complex assets pending a final order that the asset be either returned or confiscated. At minimum, the TCIM should provide investigators with contacts points for who may be consulted to take over the custody and management of a seized asset or to provide guidance on measures to avoid loss of value of frozen assets. This may vary depending on the nature and complexity of the asset(s) involved (for example, management of a seized aircraft will differ to the management of frozen bank account). For more detailed advice on global best practices, see *Managing Seized and Confiscated Assets: A Guide for Practitioners* (Bostwick et al., 2023[16])

Asset confiscation

Unlike asset freezing and seizing, which are provisional measures, confiscation of assets, can be defined as "the permanent deprivation of assets by order of a court or other competent authority" (UNODC, 2004[17]) The legal frameworks for asset confiscation (which may also be referred to as asset forfeiture) vary between jurisdictions, as does the scope of the assets that may be confiscated. Some of these differences are described below. The TCIM should inform investigators of the legal basis and procedures in place in

their jurisdiction, and as always, reference all relevant legislative provisions, and provide links to templates/checklists for asset confiscation applications.

Legal avenues for asset confiscation

Jurisdictions offer diverse avenues for the recovery of assets which could be criminal, civil, or administrative in nature. Moreover, the proceedings might be either completely domestic (for crimes committed and assets located in the jurisdiction), or first domestic then followed by a formal request to a foreign jurisdiction to enforce the order (where the assets are held abroad) (see section 20 below). Alternatively, the proceedings may be initiated at the request of a foreign jurisdiction seeking to enforce its own confiscation order. Some jurisdictions provide for administrative confiscations. Depending on the legal avenue, different provisional measures outlined in the above section may be available to prevent the dissipation, concealment, or transfer of assets pending a court's ultimate decision on whether or not to approve a confiscation order.

In practice, the two most common forms of confiscation are conviction-based confiscation and non-conviction-based confiscation (with some jurisdictions offering both) (Bostwick et al., 2023[16]). The key differences between the two regimes are outlined in the table below. Both should be viewed as complementary tools in the recovery of assets. The TCIM should make clear whether either or both regimes are applicable and when and how each should be utilised in a criminal tax investigation.

Table 6. Key differences between conviction and non-conviction based asset recovery regimes

Description	Conviction based	Non-conviction based
Legal basis	Requires a criminal conviction before an asset confiscation order can be made.	Allows for confiscation without the need for a criminal prosecution or conviction. The action is taken against the asset itself and not the individual.
Purpose	To remove criminal proceeds, instrumentalities, or corresponding value from convicted offenders.	Focuses on the illegal nature of the assets themselves, independent of any criminal proceedings.
Evidentiary threshold	The criminal standard of 'beyond reasonable doubt' or a lowered standard, applied specifically for the confiscation proceeding, once the defendant has been found guilty of an offence at a higher threshold.	Usually a civil standard such as 'balance of the probabilities' or 'preponderance of the evidence' and which may entail a reversal of the burden of proof once an initial showing is made by the government or other mechanisms such as a showing of unexplained wealth (the legal origin of the property must then be proven).
Application	Applied upon conviction (e.g. for a tax or other financial crime).	May be used in several situations, e.g. where there is insufficient evidence for a criminal conviction or the statute of limitations has expired. It can also be used for more practical reasons, such as the suspect is dead, cannot be found, their identity is unknown, or the offender is immune from prosecution.
Procedural mechanism	Integrated within or after a criminal trial.	Typically this would be carried out as part of an independent civil or administrative law proceeding (whether direct seizure by authorities using statutory powers, production of an unexplained wealth order requiring the owner to justify the origins of the asset (see box 19), or an independent lawsuit targeting the asset).

Source: OECD (2025)

Box 19. Use of unexplained wealth orders in the United Kingdom

Unexplained wealth orders (UWO's) require people or organisations to explain how they obtained property.

UWO's were introduced to the UK's Proceeds of Crime Act in 2017 and expanded in 2022 in response to the Russian invasion of Ukraine.

In the UK, all five enforcement agencies in England and Wales can apply to the High Court for a UWO where there are reasonable grounds for suspecting that a respondent – an individual or organisation – holds property (with a minimum combined value of GBP 50 000); and either that:

- their known sources of lawfully obtained income would have been insufficient to obtain the property in question; or
- that the property was obtained through unlawful conduct.

The UWO requires the respondent to explain their interest in property, how they came to obtain it, and any other information required by the order.

UWOs may be served on two categories of respondent:

1. politically exposed persons (PEPs) (as defined in the act) and
2. persons reasonably suspected of involvement in, or of being connected with persons involved in, serious crime.

If the respondent is not an individual, a UWO may also be sought in respect of a 'responsible officer'.

When applying for a UWO, the enforcement authority may also seek an interim freezing order (for up to 186 days) to prevent the property under investigation being sold and provide enforcement authorities time to review material provided in response to a UWO without a concern that the property in question will be dissipated.

If a respondent fails to respond to a UWO without a "reasonable excuse", the property in question will be presumed to be recoverable in civil asset recovery proceedings. Information provided in response to a UWO cannot generally be used in criminal proceedings, except where false or misleading information is provided, in which case, the respondent may be liable to imprisonment or a fine, or both.

Use of UWO's in practice

The UK notes that the number of UWO's applied for and obtained since their introduction is low (e.g. just two were applied for in the 2023-2024 reporting period). However, it emphasizes that this must be seen within the context that they are only intended for use in exceptional and complex cases where there is no clear link between the property and unlawful conduct and where the respondent has accrued assets that cannot be explained by their known income or employment. To that end, they are an investigative tool that aims to assist agencies to gather crucial evidence at the outset of an investigation where they may otherwise be unable to do so.

If there is evidence that the property is gained through unlawful conduct, the enforcement agency can commence a civil recovery without the need for a UWO. **In the 2022-2023 reporting period, GBP 62.9 million was recovered using civil recovery orders.**

Agencies also have a range of alternative powers to use to gather information in support of asset recovery proceedings. UWOs are considered in some cases where they could be used to degrade the support structures of serious criminals and organised crime groups.

UWOs remain powerful tools to investigate those who look to use, move or hide their proceeds of crime in the UK or overseas. Even a single UWO may have a high impact. **For instance, a UWO used in one investigation resulted in the subsequent recovery of almost GBP 10 million; while in a separate investigation a UWO resulted in the recovery of GBP 14 million.**

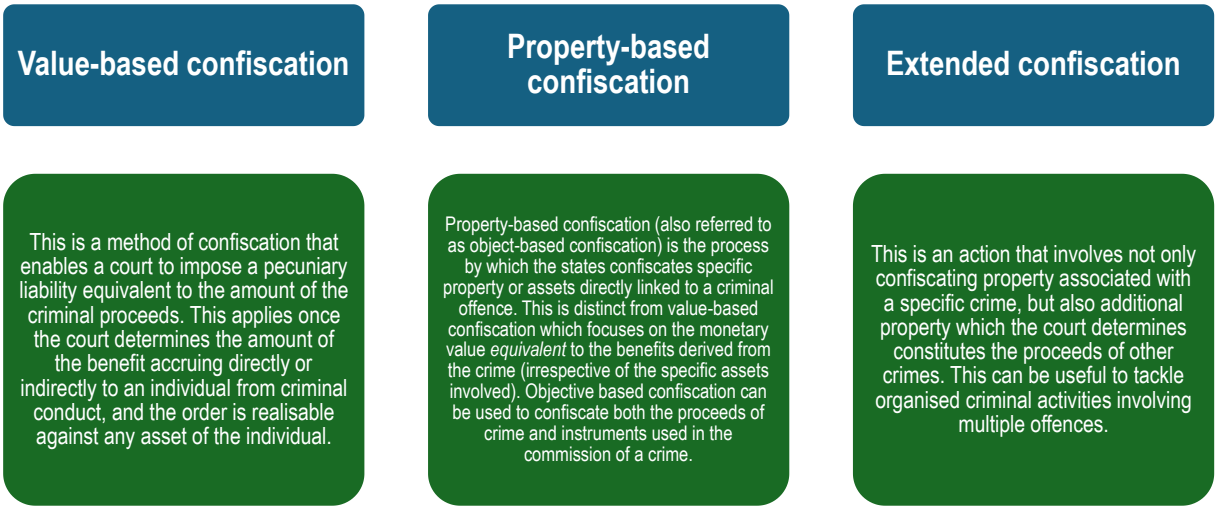
Source: www.gov.uk/government/publications/unexplained-wealth-orders-2023-to-2024-annual-report

Scope of asset confiscation

In addition to defining the legal framework for asset confiscation, the TCIM should also define what assets can be confiscated and from whom.

Beyond powers to confiscate assets held or controlled by an offender/defendant, authorities should also have powers to confiscate assets from a non-bona fide third party (i.e. a third party who is in possession of assets which are knowingly transferred to him/her by the offender to frustrate confiscation). Third party confiscation can alleviate the risk of loss due to the suspect transferring criminal property to a third party to avoid confiscation. In terms of the types of assets that can be confiscated, there are three major categories, set out in the table below.

Figure 9. Types of asset confiscation



Source: OECD (2025)

Asset confiscation procedures

Similar to the above section on asset freezing and seizing, the TCIM should reference all relevant legal provisions (e.g. under proceeds of crime legislation etc.) and outline the key elements to be included in any applications and/or orders for asset confiscation. Common elements include:

- Details of the person who is the subject of the order or warrant (e.g. the offender or a third party).
- Details of legal basis for the order (e.g. specify the details of the conviction or non-conviction based grounds.
- Detailed description of each asset to be confiscated (e.g. cash, real-estate, vehicles, bank accounts, securities, virtual assets, etc.).
- Details of the current location of the asset (e.g. whether in-country or abroad).
- Details of the current ownership of the asset including any known third-party claims to the asset.
- Clarify the process for third parties to make a claim of ownership or contest the confiscation.
- An accurate valuation of each asset (or in the case of value-based confiscation, the total monetary value to be recovered).

- Explanation of the connection between the assets and the alleged crime, including the methodology used for calculated the benefit derived from the criminal conduct.
- Mechanisms available for challenging the order (e.g. by demonstrating lawful origin).
- Measures for cross-border enforcement in the case of assets held abroad.
- Plan for how confiscated assets will be managed pending final disposition.

Enforcement of confiscation orders

In most jurisdictions, the disposal and ultimate use of the confiscated funds or assets will be defined by law and may be subject to certain processes (e.g., opportunities for victims to make claims, considerations of international sharing, or other lawful purposes as set out by law). In some circumstances, this may be included in the confiscation order. The most critical process post-issuance of this order is for the authorities to enforce the order by realising or taking final possession of the asset and liquidating it if necessary. While the end-result is likely beyond the role of a tax crime investigator, it can be useful to outline the jurisdiction's ultimate goal of asset recovery procedures in the TCIM, to ensure investigators are aware of the importance of integrating asset recovery procedures from the outset of an investigation. Common uses include:

- **Official use:** Whereby a government agency takes ownership of the asset for official use (for example, a law enforcement agency may confiscate a vehicle for use in undercover operations, prisoner transport, etc.)
- **Social reuse:** The authorised transfer to a government agency or an NGO to support social projects (e.g. transforming land or property into public parks or community centres, etc.)
- **Victim compensation or return to prior legitimate owners:** Through various domestic authorities.
- **International sharing or asset return:** May be agreed between countries pursuant to treaties or other agreements and often occurs when the recovery is the result of coordinated law enforcement action. May also result be an option where victims or other beneficiaries are located abroad.
- **Asset recovery fund:** This may be established by law for the deposit of all or a portion of confiscated property for dedicated use by law enforcement, health, education, or other purposes.
- **Salvage, scrap or destruction:** In some instances, the asset may be contraband or have no real value and the most efficient option is the disposal of them via salvage, scrap or destruction (Bostwick et al., 2023[16])

Box 20. Useful global resources on asset recovery in tax and other financial crimes cases

- Guidelines for the Management of seized assets (Council of Europe, 2023[18])
- Asset Recovery Guidance and Best Practices (FATF, forthcoming late 2025)
- Recovering International Proceeds of Crime through Inter-Agency Networks (FATF, 2023[19])
- Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery (FATF, 2012[20]) (updated version due late 2025).
- Civil Society Organisations & Asset Recovery - A Manual for Action (CiFAR, 2022[21])
- Orders without Borders: Direct Enforcement of Foreign Restraint and Confiscation Decisions (Betti, Kozin and Brun, 2021[22])
- Revised Draft Non-binding Guidelines on the Management of Frozen, Seized and Confiscated Assets (Secretariat to the UNCAC Conference of State Parties., 2018[23])
- Effective Management and Disposal of Seized and Confiscated Assets (UNODC, 2017[24])
- Asset Recovery Handbook: A Guide for Practitioners, Second Edition (Sotiropoulou et al., 2021[25])
- Managing Seized and Confiscated Assets: A Guide for Practitioners (Bostwick et al., 2023[16])

18 Interview and inquiry

Interviews are used to obtain leads, develop information, and secure evidence. The testimony of witnesses and the confessions or admissions of alleged perpetrators are major factors in resolving tax investigations. Generally speaking, there are three types of interviews that are conducted for the purposes of a tax crime investigation.

- Suspect interview
- Witness interview
- General interview (to provide information for the investigation)

Difference between an interview and an inquiry

A civil/administrative inquiry (where a taxpayer is typically compelled to respond) and an interview under caution are two distinct processes used to investigate during a tax audit, while the latter is employed during a criminal tax investigation. The table below highlights broad differences between the two processes. However, each jurisdiction's TCIM should identify in detail, the practical and legal differences between the two and when how each process should be employed.

Table 7. Basic differences between interview and inquiry into a person's tax affairs

	Civil Inquiry	Interview under caution
Interviewing authority	Conducted by tax authorities.	Conducted by law enforcement authorities (which depending on the jurisdictions may sit within or outside of the tax administration)
Purpose	To investigate a persons' tax affairs for the purpose of determining whether there is an outstanding tax liability.	To question the taxpayer about suspected criminal activity.
Scope	Often broad in scope capturing all aspects of a person's tax affairs.	Typically focused specifically on the offences the taxpayer is suspected of having committed.
Rights of the individual	Taxpayers are typically compelled to co-operate with an inquiry and will face penalties for non-co-operation.	The taxpayer has specific legal rights, including the right to remain silent and the right to legal representation.
Legal implications	Information uncovered during an inquiry can typically only be used for civil/administrative purposes.	Information obtained under interview can be used as evidence in criminal proceedings.
Process	Typically begins with a notification and is a less formal process that can involve various means of communication.	Formal process, usually recorded, and structured according to the jurisdiction's criminal procedure code/laws.
Timing	Typically conducted earlier in an investigation.	Often conducted later in an investigation once initial inquiries into the persons tax affairs have raised suspicions of criminal offender.

Suspected criminal activity uncovered during an inquiry

In most cases a civil inquiry uncovers suspected criminal conduct, the case will be referred to the authority mandated to conduct criminal tax investigations. Depending on the jurisdiction's legal framework, this may be a different team within the tax administration or an external law enforcement authority such as the police, prosecution, or a specialised financial crime agency (see section 24 for more information on reporting and sharing between civil and criminal tax authorities). Once referred, information gathered after the referral must be kept separate from the criminal investigation (see Box 13 & Box 14 above). Depending on the jurisdiction, information obtained before the referral may be used in the criminal investigation. The sections below cover the various elements of interviews in criminal tax investigations.

Responsible authority

The TCIM should identify which authority is responsible for conducting suspect interviews and the law underpinning this authority. Further, it should identify the individual(s) within the tax crime investigation authority who has ultimate responsibility for approving and summoning a person for an interview.

Initial contact

Before reaching out to an individual for an interview, it is important to assess the potential demeanour of that person during the process, in particular whether they are likely to be friendly, hostile, or indifferent.

- **Friendly:** A friendly witness is someone who willingly co-operates with the investigation. There can be various reasons why witnesses are friendly. However, it is crucial to note that even if a witness appears co-operative, it is still important to ascertain their relationship with the accused to ensure there are no hidden motives or personal vendettas against the accused.
- **Reluctant or hostile:** This describes an unco-operative individual who is often a friend or associate of the suspect. The witness may also display hostility due to their own involvement or guilt in the criminal activity being investigated.
- **Neutral:** This refers to an impartial third party, such as a custodian of a government office. This individual has no personal stake in the investigation's outcome and provides objective information or documents.

To increase the likelihood of both attendance and co-operation during an interview, it is recommended that the interviewing authority make initial contact with the individual prior to issuing the formal summons order or request. This is particularly the case with respect to suspects who may exhibit reluctance or hesitation in responding to the formal summons.

Preparation and delivery of a summon order

An interview summons is a formal document issued by a responsible authority (i.e. tax or law enforcement) to appear for questioning. The TCIM should include detailed information on:

- Accessing the summons form (include links to a template);
- Completing the summons form. Typically, it will include information about the individuals being summoned, type of summons, relationship to the business, and purpose of the summons, time, date, and location for the interview, information for the person on steps to follow if they have due cause for non-attendance (e.g. ill health);

- The approvals process, including the respective persons responsible for preparing and approving the request;
- The method for delivery of the summons (e.g. hand delivered to the individual/entity at least 24 hours prior to the time mentioned in the order).

Planning an Interview

Interviewing plays a pivotal role in the process of conducting a criminal investigation. By carefully planning an interview, time can be saved, and the direction of the interview can be effectively managed. This enables the investigation team to be better equipped to counter any false information that a suspect or interviewee might present during the interview, thus enhancing the overall effectiveness of the investigation process. The TCIM should identify who is responsible for preparing and signing off on an interview plan, as well as links to any templates developed for this purpose. At a minimum, an interview plan should cover:

- Points to prove
- Potential defences
- Facts already established
- Facts to be determined

While topics covered in an interview will necessarily differ depending on the individual being summoned, their role in the business, and the nature of the offence(s) under investigation, a typical interview would generally cover:

- The business operation
- The interviewee's role within the business
- Records management
- Documentation
- Key individuals involved
- Return preparation and filing.

In the case of witness interviews, it is always important to understand the relationship between the witness and the accused, to put the information provided by the witness into context.

Legal warning

The TCIM should clearly state the point at which a suspect being interviewed must be informed of their legal rights. This will vary from jurisdiction to jurisdiction. For example, in many jurisdictions, law enforcement is not required to inform individuals of their rights in casual encounters or general questioning. However, there will be obligation to inform suspects of their rights at specific stages of interaction with law enforcement, including when the individual is:

- **Being held in custody** (e.g. suspect is in custody for the purposes of interrogation or becomes a suspect while in custody, then the warning must be given prior to any questioning).
- **Under arrest** (the warning is typically given at the time of arrest).
- **Formally questioned about a suspected offence** (i.e. any interview where law enforcement intends to question the suspect on matters that are intended or likely to elicit an incriminating response).

The TCIM should also clearly state the details of the legal warning and the processes for issuing the warning. Typically, they should be both read aloud and communicated in writing to the suspect(s) under summons each time that the individual/entity is being summoned for questioning. It is also recommended the TCIM include a link to templates for the written warning and a text of the verbal warning. At a minimum, a legal warning should inform a suspect of:

- The details of the charges or allegations against the suspect.
- The suspected offence(s) with legal reference.
- Their right to remain silent and not to provide any details other than confirming identity.
- Their right to refuse to answer specific questions.
- The fact that any testimony provided could be used in court against the individual/entity.
- Their right to legal counsel.
- The suspect's right to state sponsored legal counsel, if the suspected offense(s) is/are serious and the person under summon does not have the financial means to obtain legal counsel (see below).
- Their right to interpretation and/or translation services.

Right to counsel

As outlined above, anyone under arrest or summons for a tax crime must be notified of their right to employ legal counsel. This should be communicated in any formal summons, at the time of arrest, and communicated again prior to commencing an interview. The TCIM should provide detailed guidance on:

- The process to follow where the suspect wants to appoint their own lawyer (including links/templates they are required to complete e.g. with the lawyer's name and licensing details, etc.);
- The process to follow where the suspect needs a state-appointed lawyer;
- The time periods allowed for the suspect to appoint a lawyer (e.g. 24-48 hours);
- How to request an extension where the suspect is unable to appoint a lawyer within the allocated timeframe.
- The process to follow where the lawyer does not meet the eligibility requirements set out in the jurisdiction's law (e.g. does not hold a valid practicing certificate, has been suspended, is linked to the investigation, recently employed at the tax administration, etc.).

Interpretation and translation services

It is mandatory in the vast majority of jurisdictions that accused persons can understand information about the criminal proceedings in their own language. This ensures that language barriers are not an obstacle to a fair trial. Thus, the accused has the right to interpretation and translation by a representative of the state authority, during questioning, any pre-trial meetings between the prosecution and the accused and their lawyer, and during all court appearances and hearings.

The TCIM should clearly state the process for obtaining interpretation or translation services, including links to any directories, contact points, request forms, etc.

Interview process

In addition to ensuring the individual is aware of the purpose of the interview, informed of their legal rights, and has access to interpretation services, the TCIM should also outline any other factors that are relevant to the interview process. Examples of other factors could include:

- Ensuring that children (as defined by law) are accompanied by a parent, guardian, or individual who can protect the child's rights;
- Ensuring the individual is given sufficient breaks from continuous questioning (as defined in law);
- Ensuring that the entire interview, including the orally communicated legal warning, questions, and answers, are recorded (either orally or via video);
- Informing individuals that the recordings can be admitted as evidence during any subsequent court proceedings, as applicable in each jurisdiction's law.

Investigation statement and transcript

Depending on the jurisdiction, the investigation team may prepare a written statement based on answers provided during an interview, or a verbatim transcript for internal purposes. For either approach, the TCIM should identify the process, including who is responsible for preparing and approving the statement. Generally speaking, a written statement should:

- Include any significant evidential points;
- Be accurate and specific;
- Be confined to an account of those parts of the interview which are directly relevant in evidential terms both to the prosecution and the defence;
- Be checked for accuracy/grammatical errors.

The TCIM should also include links to any templates or forms for the written statement, that should, typically, include, the following information:

- Details pertaining to the identity of person/entity making the statement.
- Summary of the offences in respect of which the statement is taken.
- A confirmation that the right to legal counsel had been granted.
- If the person is an alleged suspect that the right to remain silent had been provided;
- Information provided by the person summoned.
- A declaration from the person/entity under summons that the information provided to the investigation is accurate and true.
- Date, time and place of the statement made by the person.
- Signature (and in some cases fingerprint) of the person providing the testimony, the Manager/ or Case Officer who conducted the interview, and the eyewitnesses who were present when the statement was recorded, if any.

In most jurisdictions, once a statement has been approved internally, it needs to be signed and validated by the person who provided the testimony. To that end the TCIM should outline the internal process for signature (e.g. prepare 3 copies of the statement and invite the interviewee to sign/validate the statement on each page). Where the person refuses to sign the statement or does not respond to requests to sign the statement, this should be stated therein.

19 Arrest

Arrest refers to the power granted to law enforcement authorities to stop, restrain, and take a person into custody for the purpose of formally charging them with a criminal offence. This is an important power in criminal tax investigation to prevent suspects influencing other suspects or witnesses, becoming a flight risk, or committing additional crimes.

As with all enforcement powers, the TCIM should clearly state what law enforcement agency or agencies are mandated to arrest suspects, and outline the procedures, safeguards, and authorisation mechanisms in place to prevent potential abuse of these powers. At a minimum, the manual should guide investigators on the relevant laws and procedures that apply to:

- **Establishing probable cause** (i.e. having reasonable grounds to suspect that a person has committed or is committing a crime based on direct observation and/or evidence gathered).
- **Initiating arrest** (generally speaking officers should identify themselves, inform the person that they are under arrest and for what crimes, and make clear that the person is not free to leave);
- **Use of force** (i.e. only when necessary to carry out the arrest and should be restricted to the least amount possible);
- **Informing the suspect of their rights** (e.g. right to remain silent, legal representation, etc. Refer also to the guidance on legal warnings in section 19 above);
- **Search and seizure** (for example, a pat down to check for weapons, evidence and/or contraband);
- **Transportation and booking** (i.e. the process for where the suspect will be taken and details of the booking process e.g., photographs, fingerprints, etc.);
- **Other legal rights and procedures** (e.g. the right to appear before a judge within a certain timeframe prescribed by law).

20 International co-operation

International co-operation in cases involving tax and other financial crimes can take a number of forms, both formal and informal. The TCIM should outline the procedures, benefits, and drawbacks of all forms of cross-border co-operation so authorities can determine the most appropriate form of co-operation to use at different stages of an investigation (e.g. intelligence gathering, evidence gathering, recovery of assets etc.).

Informal cross-border co-operation

Informal cross-border co-operation in criminal tax matters refers to direct collaboration between competent authorities in different countries used pursuant to treaty or other legal arrangements and may occur outside of the formal channels for mutual legal assistance or mutual administrative assistance. It is important to note that informal co-operation is intended to complement (and not replace) formal co-operation mechanisms in urgent and time sensitive situations.

Unlike formal mechanisms that must be underpinned by a legal instrument and follow specific (and often time consuming) procedures, informal co-operation relies on less stringent agreements and/or mutual trust among the parties involved. For example, informal exchange of financial intelligence between FIUs via Egmont Group requests can support the detection of suspicious transactions linked to tax evasion schemes and support the tracking of IFFs. Likewise, law enforcement liaison officers or attachés from revenue agencies stationed abroad can be valuable sources of information for co-operation.

As with all international co-operation, informal co-operation also has some drawbacks. For example, many jurisdictions will have restrictions in place for what types of information may be shared outside of formal channels. To that end, where informal co-operation is used, the TCIM should specify what types of information may be shared informally, and through what channels, noting that it is critical that sensitive and confidential information remains secure, even when shared informally.

Informal co-operation offers a range of benefits including:

- **Speed/efficiency:** Informal co-operation can take place through direct and informal channels such as phone calls, emails or instant messaging, bypassing the cumbersome formal co-operation channels often involved with formal legal processes. This is particularly useful in urgent and time sensitive situations, which is increasingly important noting the speed and ease with which criminals can now operate across borders.
- **Enhanced intelligence gathering:** Informal co-operation is most useful during the intelligence gathering stages of a case, to help steer investigators towards valuable evidence to be obtained through formal channels as the case progresses towards prosecution.
- **Co-ordinated actions:** Informal co-operation can be the catalyst for the establishment of joint cross-border investigations, taskforces, or joint investigation teams.

- **Improved investigative capacity:** Sharing of expertise, techniques, and experiences among authorities leads to improved ability to detect, investigation, and prosecute tax and other financial crimes.
- **Building trust:** Informal co-operation is a useful way to foster trust among competent authorities, leading to increased likelihood for more effective and efficient formal co-operation at the evidence gathering stage.

Box 21. Enhancing cross-border collaboration through the Global Tax Crime Enforcement Network

In May 2024, the OECD hosted a pilot meeting of the Global Tax Crime Enforcement Network (TCEN). The aim of the proposed network was to provide a platform for annual in-person confidential discussions to take place between heads of tax crime and others involved in investigations related to tax crime on practical operational issues, whether general in nature or related to specific cases.

The purpose of the network is not to create new policy initiatives, political declarations, or any other outcome documents, but rather to enhance operational capabilities, and where relevant, to share insights to feed into the policy agenda. The core objectives of the network are set out below. If your jurisdiction is interesting in joining the network, please reach out to OECD.TaxandCrime@oecd.org.

Formal cross-border co-operation

Unlike informal collaboration, formal cross-border co-operation among tax and other law enforcement authorities is governed by legal instruments such as bilateral or multilateral treaties or memoranda of understanding. This can take a number of forms including exchange of information and information sharing, service of documents, obtaining evidence, facilitating the taking of testimony from witnesses, transferring

persons for questioning, executing asset freezing and seizing orders (including enforcement of judgments), and joint investigations. However, for such co-operation to take place, there must be an underlying legal basis that sets out the terms and procedural requirements co-operation such as a treaty or the principle of reciprocity.

When it comes to international co-operation on tax crimes, many law enforcement authorities default to use of bilateral or multilateral Mutual Legal Assistance (MLA) treaties overlooking the availability and power of tax exchange of information (EOI) instruments. While it is of course up to each jurisdiction to determine what instrument to use for sending/requesting information in each case, it is well known that traditional MLA procedures can be cumbersome, time consuming, and slow. This is particularly problematic when investigating criminals who can move vast sums of money across borders in real-time. To that end, the TCIM should educate investigators on when and how EOI might be used as an alternative to, or in combination with, MLA procedures.[5]

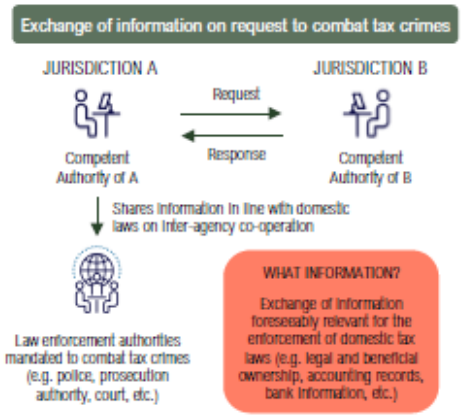
To support effective use of international co-operation in practice, the TCIM should include information on:

- **The underlying legal framework for MLA in criminal tax matters** including links to any bilateral and multilateral agreements/treaties in place;
- **The underlying legal framework in place for EOI in criminal tax matters,** including links to the Convention on Mutual Administrative Assistance in Tax Matters ("the MAAC") and any bilateral or multilateral Tax Information Exchange Agreements and Double Tax Agreements to which the jurisdiction is a Party;
- **The respective competent authorities for all EOI and MLA agreements in place**, including contact points for the relevant individuals and/or units through whom requests should be sent and received.
- **How information can be exchanged,** for example, under the MAAC information can be exchanged **upon request** of another jurisdiction, **spontaneously** (where foreseeably relevant to another jurisdiction for tax purposes, or **automatically** (i.e. the annual automatic exchanges between tax authorities using the OECD's Common Reporting Standard which defines what information is shared automatically (e.g. on the legal and beneficial owners of financial accounts, and the assets held, and income received, on such accounts)).
- **The types of information that can be exchanged under relevant MLA and EOI instruments** (e.g. the MAAC provides for the exchange of any information that is "foreseeably relevant" to the enforcement of any taxes, including any tax crime).
- **Procedures for international co-operation via MLA and EOI.** This should include practical information on the internal processes to follow to initiate and/or respond to a request for international co-operation in criminal tax matters including contact points within the competent authorities and templates for sending and/or responding to requests.
- **The TFTC's database for International Co-operation in Criminal Tax Matters:** The TFTC maintains a secure database of easy to access contact points for international co-operation in criminal tax matters through both EOI and MLA instruments. The database is accessible to competent authorities of all jurisdictions that have themselves provided inputs. If you are a competent authority who is interested in gaining access to the database, please contact OECD.TaxandCrime@oecd.org.

[5] Flyer: The Power of Exchange of Information Agreements for Law Enforcement Authorities: https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-and-crime/flyer-power-exchange-of-information-agreements-for-law-enforcement-authorities.pdf

Figure 10. The power of EOI agreements in combatting tax crime

USE OF EOI AGREEMENTS TO COMBAT TAX CRIMES IN PRACTICE



In many jurisdictions, the tax administration is not the authority mandated to combat tax crimes and other financial crimes (e.g. in many jurisdictions, it is the police or prosecution authority who investigates, prosecutes, and/or recovers the proceeds of financial crimes). To that end, tax administrations around the globe have varying arrangements in place to enable them to share taxpayer information with domestic law enforcement authorities for the purposes of combatting tax and other financial crimes. This can range from tax administrations being able to provide information to domestic law enforcement authorities spontaneously or on request, or in some jurisdictions, law enforcement authorities being granted access to the tax administrations' database.

Similarly, EOI agreements contain secrecy provisions that mandate when and how tax administrations can share information received via EOI instruments with other domestic financial crime authorities to combat tax crimes and other (non-tax) related serious financial crimes.

ABILITY OF TAX ADMINISTRATION TO SHARE EOI DATA WITH DOMESTIC LAW ENFORCEMENT AUTHORITIES TO COMBAT TAX CRIME

In general, provided a tax administration can share information with its domestic law enforcement authorities for the purposes of combatting tax crimes under its domestic law, it may share information obtained from a foreign tax authority pursuant to an EOI agreement in the same manner. The provisions on confidentiality of information exchanged are found in Article 26(2) of the OECD Model Tax Convention, Article 8 of the Model TIEA, and Article 22 of the MAAC, and provide, more specifically, that the exchanged information should be protected in the same manner as information obtained by tax administrations under their domestic laws. The provisions further provide that information may be shared with persons or authorities concerned with the enforcement of tax laws, including law enforcement authorities, courts, administrative, or supervisory bodies that are concerned with the investigation, prosecution, and recovery of assets linked to tax crimes. Notwithstanding these provisions, information may also be disclosed in public court proceedings or in judicial decisions relating to such taxes.

ABILITY OF TAX ADMINISTRATION TO SHARE EOI DATA TO COMBAT OTHER (NON-TAX) RELATED SERIOUS CRIMES

As a notable exception to the rule that exchanged information must be only used for tax purposes, it can be used to fight other serious crimes, including money laundering terrorism financing, bribery, corruption. For example, the 2012 update to Article 26(2) of the OECD Model Tax Convention and Article 22(4) of the MAAC provide for use of EOI data for such "non-tax" purposes if it is allowed under the laws of both States and the competent authority of the supplying jurisdiction authorises such use. In practice, this means that where the domestic laws of both jurisdictions allow for information sharing between the tax administration and law enforcement authorities for non-tax purposes, information exchanged through EOI agreements may be shared in the same manner. Importantly, this is conditional on the competent authority of the supplying jurisdiction providing prior explicit authorisation for the wider use of the information in a particular case.

Source: OECD (2023) Flyer: The Power of Exchange of Information Agreements for Law Enforcement Authorities (https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-and-crime/flyer-power-exchange-of-information-agreements-for-law-enforcement-authorities.pdf)

Box 22. Effective use of EOI agreement to combat tax crime in Italy

In the course of a tax audit against an Italian company purchasing large quantities of pallets, the investigating local unit of the Guardia di Finanza - placed in the North of Italy – forwarded, through the provided formal channels, a request for mutual administrative assistance pursuant to the Convention against double taxation and Directive 2011/16/EU – in order to verify, for the tax years of interest, whether certain commercial transactions between the aforementioned Italian company and a supplier company based in the requested EU Member State had taken place.

Thanks to banking and tax information (current accounts and tax returns), as well as commercial and corporate documentation (invoices and chamber of commerce extracts) provided by the foreign tax Authority, the GdF local unit established:

- the inexistence of the transactions accounted by the Italian company audited and the non-deductible related costs, resulting from the use of invoices for non-existent transactions and amounting to more than EUR 1.3 million and more than EUR 300 000 of evaded tax;
- that the two *de facto* administrators of the Italian company (Italian entrepreneurs with family ties) had intentionally set up the foreign company, supplier of pallets, whose seat was also that of two other foreign companies of which the aforementioned entrepreneurs were the beneficial owners;
- the criminal-tax violations provided for in Articles 2 *('Fraudulent declaration through the use of invoices or other documents for non-existent transactions')*, 3 *('Fraudulent declaration through other artifices')* and 8 *('Issuance of invoices or other documents for non-existent transactions')* of Legislative Decree 74/2000 (Italian legislation on tax crimes), which were reported to the competent Judicial Authority.

Moreover, the investigations carried out by the GdF operating unit showed that the foreign business enterprise based in the requested EU Member State was used for the systematic laundering of proceeds obtained in Italy through the issuance of invoices for non-existent transactions.

In this context, the information provided by the foreign Tax Authority - who was asked for the consent to use the data obtained for purposes other than tax purposes (assessment of money laundering offences) - was useful to prove that the laundered proceeds, amounting to over EUR 2.5 million, were transferred to foreign bank accounts and to ascertain the execution of cash withdrawals, on a weekly basis, which allowed these illicit funds to be brought back into Italy.

Source: Guardia di Finanza, Italy (2025).

Box 23. Useful global resources for international co-operation in criminal tax matters

To aid law enforcement authorities in making full use of EOI instruments, the OECD has prepared the below (non-exhaustive) list of resources that provide comprehensive information on when and how EOI can be used in cases involving tax and other financial crimes.

Relevant information on international standards on tax transparency and exchange of information

- Global Forum Model Manual on Exchange of Information for Tax Purposes, https://www.oecd.org/tax/transparency/documents/model-manual-on-exchange-of-information-for-tax-purposes.htm
- Global Forum on Transparency and Exchange of Information for Tax Purposes, https://www.oecd.org/tax/transparency
- Key guidance, toolkits, and documentation of the Global Forum, https://www.oecd.org/tax/transparency/documents/key-publications-and-documents.htm
- OECD's e-learning in taxation, https://www.oecd.org/en/about/programmes/global-relations-programme-on-taxation/self-paced-training.html

Legal text and commentaries on the MAAC

OECD and Council of Europe (2011), The Multilateral Convention on Mutual Administrative Assistance in Tax Matters: Amended by the 2010 Protocol, OECD Publishing, https://dx.doi.org/10.1787/9789264115606-en

- The text of the Amended Convention in English, French, German (unofficial translation), Spanish (unofficial translation) and Portuguese (unofficial translation), https://www.oecd.org/en/topics/convention-on-mutual-administrative-assistance-in-tax-matters.html
- The Revised Explanatory Report to the Convention on Mutual Administrative Assistance in Tax Matters as Amended by 2010 Protocol, OECD/Council of Europe (2011), *The Multilateral Convention on Mutual Administrative Assistance in Tax Matters: Amended by the 2010 Protocol*, OECD Publishing, Paris, https://doi.org/10.1787/9789264115606-en (page 31).

General information on the MAAC

- OECD Convention on Mutual Administrative Assistance in Tax Matters: https://www.oecd.org/en/topics/convention-on-mutual-administrative-assistance-in-tax-matters.html
- Chart of participating jurisdictions (signatures and entry into force): https://www.oecd.org/content/dam/oecd/en/topics/policy-sub-issues/convention-on-mutual-administrative-assistance-in-tax-matters/status_of_convention.pdf
- List of declarations, reservations and other communications: Multilateral Competent Authority Agreements for automatic exchange of information, www.coe.int/en/web/conventions/fulllist?module=treaty-detail&treatynum=127
- Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information (the "CRS MCAA"), for the automatic exchange of financial account information pursuant to the Common Reporting Standard: https://www.oecd.org/en/topics/sub-issues/international-standards-on-tax-transparency/tax-transparency-resource-centre.html

21 Investigation case file

A well organised investigation case file is the backbone of an effective tax crime investigation. It serves as a detailed record of tasks that have been or will be carried out over the course of the investigation process and the outcomes of those measures. An investigation case file should be a living document from the beginning to the end of an investigation. This part of the TCIM should stress the importance of maintaining a comprehensive and up to date case file, noting that this is critical for:

- Effective evidence organisation and management;
- Compliance with legal requirements and facilitating proper disclosure;
- Supporting prosecutors in preparing the case for trial;
- Maintaining continuity in an investigation, for example, where there is a change in the investigating officer(s) or old cases are reopened;
- Quality control and supervision.
- While the contents of the file will vary from case to case, it should at a minimum, include information on the subjects outlined in the table below.

Table 8. Contents of investigation case file

Subject	Description
Case background	The case file should contain case background describing the date and way the case was reported or detected, and a clear statement of the allegations made by complaint or details of the risks highlighted.
Case summary	It should contain list of parties involved (witness/suspect) including their names, relationship with the company, and a list of all suspected offences with their specific legal reference. It should also describe the period of admissible evidence and details of the available evidence, and the legal references regarding offences committed by the suspect.
Taxpayer business background	Investigators should compile the detailed information of taxpayer's business activities including the nature of service provided by each activity, shareholder structure, and any other risk factors that could have an effect in conducting an efficient investigation.
Taxable activities of taxpayer	For example, the name, address, and operational status, and any other specific information identified pertaining to the activities related to the investigation.
Scope & objectives of investigation	Investigators should outline the scope and objectives of the investigation for planning purposes.
Investigation procedure	The procedures should be outlined regarding collecting the list of documents which the investigators believe is essential for the investigation, including document source/reference, and the types of documents collected.
Searches conducted	Detailed information on any searches conducted as part of the investigation (see also section 16 on search powers).
Evidence collected	Description of all evidence collected during the investigation whether from a search or any other source. The details of evidence collected should be disclosed in an accurate manner so that the reviewer can easily access the evidence if necessary.
Summary of any summon orders issued and conducted	Detailed information on any summons orders and interviews conducted. The summons order detail should contain information on the person for whom the order was issued, including identity, designation/relationship to taxpayer, date the summons order was issued and reasons for the issuance, as well as a summary of important information gathered. (see also section 19 above).
Findings from the summons conducted	A summary of findings from all suspect and witness interviews.

Additional tax resulting from the suspected offences	A statement of any additional tax due should be included in the case file in order to give assurance to the investigation findings and for an indication of tax evasion or other crime.
Statement of investigation officers	An analysis of the facts uncovered, and the remedial actions taken as a result should be mentioned in this section. Investigators should also highlight if criminal activity was identified during the investigation process. Based on that, investigators should give a clear recommendation of what, if any, action should be taken
Meeting log	Investigators should maintain a proper log of important events carried out during the investigation. The section should consist of all the meeting details with the taxpayer and witnesses.
Document log	This section should include a list of documents and evidence that were acquired and reviewed during the investigation including dates taken and mode of collection.

22 Financial analysis: Direct and indirect methods of proof

During criminal investigations, law enforcement authorities are required to use various methods of proof to detect and establish tax fraud or evasion. These methods are typically categorised as direct or indirect and are designed to analyse financial data, detect discrepancies, and reconstruct a taxpayer's overall finances. For example, a bank statement will rarely be proof of tax evasion, but rather contain information that requires further analysis, often in combination with other datasets that will demonstrate what a person's taxable income should have been.

Methods of proof are critical in tax and financial crime investigations given their inherent complexity, particularly in jurisdictions where tax crimes are tried by jury or judges without specialist training on economic crimes, or juries of laymen. Methods of proof are key for helping investigators identify what documents and evidence should be obtained during the information gathering stage. Moreover, they are central to a prosecution authority's case, which must comprise a strong and coherent legal argument to convince a judge or jury that a crime has in fact taken place.

Useful definitions

It is recommended that a TCIM include definitions that distinguish the differences between evidence and proof and explains the relationship between them. This should also include distinctions between direct and circumstantial evidence, as well as direct and indirect proof. This will help supplement the investigator's knowledge and provide further resources to guide their approach to the investigation. This is beneficial as some methods of proof can be used to support a legal argument where there is a lack of direct evidence regarding a suspect's income, particularly where the case involves significant amounts of physical cash, substantial unexplained asset accumulation, and/or excessive consumption expenditure is observed. The table below sets out some basic descriptions as examples. However, as always, it is important that each jurisdiction adapt these to its legal context.

Table 9. Useful definitions of evidence and proof

Key terms	*Descriptions [examples only]*
Proof	"Proof" means providing evidence that convinces the judge or jury that something is true. It is the convincing reason to believe that a statement or fact is correct. In legal terms, proof refers to all the evidence presented during a trial that follows the rules of law, with the goal of persuading the judge or jury to reach a decision or verdict.
Evidence	"Evidence" is a narrower term that refers to specific proof allowed in a trial, such as witness testimonies, records, or documents. It is the actual information presented to support or challenge a fact. On the other hand, "proof" is the outcome or result of the evidence provided. In simpler words, evidence is like the tool used to prove or disprove something, while proof is the result that confirms whether something is true or not.
Direct evidence	Direct evidence proves a fact, without an inference or presumption, and conclusively establishes that fact without reference to any supporting evidence. Direct evidence is evidence of the precise fact in issue and is distinguished from circumstantial. For

	example, transaction tracing instructions obtained from a bank prove that an account belonging to an entity remitted a specific amount to an account belonging to another entity on a particular date.
Circumstantial evidence	Facts presented from which the existence of the main fact may be logically inferred. Circumstantial evidence presents two chances for mistake: error of assertion and error of inference. For example, recurring credit transactions observed in a bank statement that are received periodically on the same day of each month and are described as “Salary” infers that the amounts may be income earned by the account holder. However, the amounts may be in fact received on behalf of another person such as in the instance where an individual has part of their salary paid into their spouse’s account.
Direct methods of proof	The direct method of proof relies on direct evidence. It is straightforward and makes it difficult for the suspect to deny the evidence. It is also the simplest method to include in an investigation report, presented in court by prosecutors, and for the judge and jury to comprehend. For example, an analysis of a bank account statement that sums the total amount of cash deposits in an account.
Indirect methods of proof	Indirect methods of proof are used when direct methods of proof are not applicable such as where a suspect’s books and records are not available. For example, estimating the income derived by a cash-only burger shop by using the amount of burger buns it ordered from suppliers in an income year as an estimate of the corresponding sales. Furthermore, it is used when a suspect is accumulating assets, spending on consumable goods and services or depositing funds into bank accounts. Tax crimes often involve individuals driven by greed, and as a result, it is usually difficult to find clear-cut "direct evidence" to prove the wrongdoing. Depending on the specific details of each investigation, the accurate taxable income of the person being investigated can be determined using either "direct" methods of proof or several "indirect" methods.

The sections below cover some common methods used in tax crime investigations to determine omitted income amounts. However, it is critical that each jurisdiction tailor its TCIM to include:

- All methods of proof available in a jurisdiction;
- Suggestions on which methods are best suited to particular situations;
- How to undertake these methods, including the technical and technology resources available in-house;
- Identification of specialist teams or subject matter experts that can either assist with or conduct the analysis;
- Where relevant, any recent precedent or examples using particular methods in court, both where the method was either accepted or rejected, to enable investigators to replicate previous best practice and to avoid known pitfalls.

Net worth/asset betterment method

The net worth method of proof relies on various financial information, such as changes in assets, reductions in liabilities, expenses, and other related data, to indirectly determine the accurate taxable income. The net worth method of proof is used when the direct method of proof cannot be applied, such as when there is a lack of direct evidence regarding the suspect's income or when the books and records are inadequate or inaccurate. It is particularly useful when investigating cases involving the accumulation of assets by the suspect.

Investigators should use evidence of financial activities and patterns to establish the correct income for tax purposes. By subtracting the suspect’s liabilities from assets, investigators can determine the net worth for the current year. Furthermore, by comparing the net worth of this year to the previous year, the increase in net worth can be assessed. Investigators can then incorporate the suspect’s living expenses for the current year to estimate current income. By deducting funds from known sources of income, the amount of money attributed to an unknown source can be ascertained.

When the investigation team determines the amount of money the suspect possesses from unknown sources, the suspect can be confronted, and an explanation and/or confession sought. Additionally, the evidence gathered can be presented in a court of law as incriminating evidence against the suspect and in some jurisdictions may become subject to non-conviction-based confiscation.

Table 10. Formula for net worth/asset betterment method of proof

	31 Dec yr. 1	31 Dec yr. 2
Assets	xxx	xxx
Liabilities	(xxx)	(xxx)
Net Worth	xxx	xxx
Prior Year		(xxx)
Net Worth Increase		xxx
Expenditures		xxx
Total Income		xxx
Known Income		(xxx)
Undisclosed Income		xxx

Source: Maldives Inland Revenue Authority (2025)

It is important that investigators document suspects' opening net worth with reasonable certainty and a likely source of income for the proceeds in question. Some common problems with this method include failure to establish a firm starting point, failure to account for non-taxable income, failure to rebut defences raised by the suspect, and failure to establish likely sources for unreported or illegal income.

Expenditure method (source and application of funds)

The expenditure method of proof focuses on analysing the suspect's expenditures to estimate their income or identify unreported sources of funds. This should be used when the suspect spends most of his/her money on consumable goods or services and maintains no reliable books or records and relies on the assumption that the suspect's expenses are funded by their income. By carefully analysing and comparing the reported income to the expenditures, investigators can identify discrepancies and potentially uncover unreported income or hidden assets.

Table 11. Formula for expenditure method of proof

Add	**Application of Funds**	
		Personal Expenditures
		Increase in assets
		Decrease in liabilities
Less	**Sources of Funds**	
		Reported Revenue
		Non-taxable sources
		Decrease in assets
		Increase in liabilities
Equals	**Unreported income**	

Source: Maldives Inland Revenue Authority (2025)

The expenditure method of proof involves the following steps:

- **Gathering expenditure data:** Collecting detailed information about the suspect's expenses, including personal expenses, bills, or rent payments, loan repayments, lifestyle expenses, travel costs, and other relevant expenditures.
- **Categorising and analysing expenses:** Categorising the expenses into different categories, such as housing, transportation, entertainment, education, healthcare, and other relevant categories. Analysing the pattern, frequency, and magnitude of these expenses.
- **Comparing expenses to reported income:** Evaluating the individual's reported income, such as business income, employment income, investments, and other documented sources of income. Comparing the reported income to the total expenditure to determine if there is a significant gap between the two.
- **Identifying unexplained or unreported income:** If the total expenditures exceed the reported income, the difference indicates potential unreported income.

It is important to note that additional supporting evidence and documentation will be required to strengthen the case and establish the accuracy of the findings.

Bank deposits method

The bank deposits method of proving income utilises bank account records to establish a suspect's understatement of taxable income. When there is no, or insufficient, direct evidence of income and/or expenses, the investigation team can still compute the unreported income indirectly using circumstantial evidence. This method is appropriate when most of the income is deposited in bank accounts.

The underlying principle of the bank deposits method of proof is straightforward. Once a suspect receives money, there are only three possible actions he/she can take: spend it; deposit it; or hoard it. By accounting for these three areas, all the funds available to the suspect can be considered. If non-income sources are eliminated, the remaining currency expenditures, deposits, and increases in cash on hand will equal corrected gross income.

The bank deposits method of proof requires investigators to conduct a thorough analysis of the deposits and cancelled checks which relate to any and all bank accounts controlled by the suspect. If the suspect reported income on an accrual basis, adjustments should be made in the bank deposits method to reflect accrued income and expenses.

Table 12. Formula for bank deposits method of proof

Taxable Income Equals	Total deposits
	Minus transfers between accounts
	Minus redeposits of cash previously withdrawn
	Plus payments made in cash
	Minus non-income deposits
TOTAL	

Source: Maldives Inland Revenue Authority (2025)

To prove unreported taxable income through the bank deposits method, investigation team must show that:

- The suspect had a business or income producing activity;
- Regular deposits of funds were made into the suspect's accounts, or into accounts over which he/she had or exercised control;
- A full investigation of such accounts was made to determine income versus non-income deposits, and
- unidentified deposits have the characteristic appearance of income (for example, the regularity of payments).

Any deposits that have not been identified as either income or non-income deposits are referred to as "unexplained deposits". If investigators can demonstrate that the unexplained deposits have the characteristic appearance of current income, such as substantial circumstantial evidence to support an illegal business, the amounts will be utilised in determining income totals.

23 Communication standards

An efficient and effective tax crime investigation relies on the investigating authority having clear standards in place for both internal communications (i.e. within the organisation) and clear rules of engagement with external parties (whether other financial crime organisations, taxpayers, the press, or other third parties. The TCIM should educate investigators on these standards and how to apply them in their daily role.

While the standards for communications will necessarily vary between jurisdictions, the TCIM should, at a minimum:

- Specify the working language(s) for both internal and external correspondence.
- Inform officers of the protocols for note-taking during internal and external meetings, briefings, etc.
- Provide links to all available templates for internal and external documents and correspondence.
- Cross-reference to any style guides for internal and external communications.
- Outline procedures for investigators to follow when receiving and responding to both internal and external requests for information (including points of contact, persons to copy, etc.).
- Provide guidance on how to classify different types of correspondence or communications in line with domestic laws or policies (e.g. highly sensitive, internal use only, publicly available, etc.)

Remind officers that even internal communications can be subject to legal and/or freedom of information requests from the public, and therefore serve as a reminder to avoid informal language, jokes, slander, etc. in any internal or external communications which could pose a risk to the agency's reputation.

Define clear rules of engagement for communications with the public, including the press (for example, in many jurisdictions all communications about an arrest or ongoing prosecution must be done through the organisation's press office).

24 Protecting suspects' rights

As outlined throughout this guide, persons subject to a criminal tax investigation should be able to rely on certain procedural and fundamental rights, which are afforded to everyone suspected or accused of a criminal act. It is therefore critical that criminal tax investigators are both aware of these rights and understand how to apply them in practice. Failure to so not only impacts the rights of an individual but can also adversely impact the investigation and prosecution of tax crime, for example, where evidence obtained becomes inadmissible in court due to the violation of rights.

These rights may be given effect in domestic law by being enshrined in a jurisdiction's constitution or bill of rights, or within criminal procedure laws. The TCIM should include:

- A clear description of the taxpayers' fundamental rights in criminal investigations/proceedings.
- The legal basis for the right.
- Guidance on how to apply the right in practice.

The below table sets out the fundamental rights that should be afforded to all taxpayers accused of committing a tax crime, as reflected in Principle 10 of the Ten Global Principles (OECD, 2021[6]), and in line with international human rights instruments (United Nations, 1948[26]). Jurisdictions are encouraged to adapt the descriptions as appropriate, including a reference to the relevant jurisprudence and to provide practical guidance to investigators on how each right should be applied in practice, for example that the suspect must be informed of the right to remain silent, orally, at the time of arrest; contact details of interpreters, free legal defence services, etc.

Table 13. Fundamental rights of suspects

Fundamental Right	Description
The right to a presumption of innocence	All persons should be considered innocent until proven guilty. That is, prior to the final judgment of a court: suspects/accused persons must not be presented as being guilty. The burden of proof sits with the prosecution while any reasonable doubts as to the guilt should benefit the accused.
The right to be advised of their rights	Investigating agencies have the obligation to advise a suspect or accused of their rights. Depending on the jurisdiction, this can be fulfilled by orally advising the person of their rights or in writing by issuing a "Letter of Rights". The content of such advice may change depending on the legal framework. However, it is common that this advice of rights includes the right to remain silent, the right to be informed of the accusations against the person and the right to access a lawyer or in some circumstances the right to free legal advice. In practice, jurisdictions may administer these rights at different stages of an investigation.
The right to be advised of the particulars of what one is accused of	Suspects or accused persons have the right to know the nature and substance of the allegations against them. Generally, this includes the elements of the offence, such as the essential aspects of the offence, details of the alleged conduct which led to the charge and, in the case of a tax crime, the alleged damage to the state. This is commonly provided to the accused prior to entering a plea in court.
The right to remain silent	An accused person has the right to refuse to comment or provide answers when questioned

	by a criminal investigator. This aims to protect the individual of interest from imbalances of power and self-incrimination.
The right to access and consult a lawyer and entitlement to free legal advice	A person subject to tax crime investigation and prosecution have a right to access legal advice. To guarantee this right, many jurisdictions provide legal representation and advice without any cost. This fundamental right is essential to a fair legal system, given the potentially serious consequences of a conviction.
The right to access documents and case material, also known as a right to full disclosure	The accused has the right to know the details of the case being argued against them, including the evidence that is favourable to them or the prosecution. This allows the accused the opportunity to prepare a solid defence.
The right to interpretation and translation	An accused person should be able to understand the information about the criminal proceedings in their own language. This ensures that language barriers are not an obstacle to a fair trial. Thus, the accused has the right to interpretation and translation usually during the questioning of the suspect or accused by a representative of the state authority, meetings between the prosecution and the accused and their lawyer, and during all court appearances and hearings.
The right to a speedy trial	All accused persons must be protected against undue delay in the resolution of a trial as this can prejudice the accused person from receiving a fair trial because evidence may become unavailable or less reliable.
The right to protection from double jeopardy (ne bis in idem).	This right protects an accused person of being tried twice for the same crime, when (i) the person has previously been found guilty and served a sentence, or (ii) the person has been acquitted by a final judgement. This right entails that the accused cannot be tried again for a less serious crime, where all the elements of that less serious crime are subsumed in the elements of the more serious crime. It is important to note that this right does not prevent successive investigations where one investigation may not have resulted in criminal charges, but a subsequent investigation commenced.

Source: (OECD, 2021[6])

25 Preparing an investigation report

Once the investigator/investigation team has concluded the case, a detailed investigation report should be approved through the appropriate channels. The TCIM should:

- Identify who is responsible for preparing an investigation report;
- Provide guidance on how to draft a report (including links to any available templates, style guides, language, etc.)
- Set out the procedures for any internal and/or external approvals required of the report;
- Provide guidance on the steps to follow if the case is being referred for prosecution;
- Provide guidance on the steps to follow if the case is not being referred for prosecution (e.g. in many instances this would result in it being referred back to civil/administrative tax authorities for an assessment of any tax liability).

Table 14. Contents of an investigation report

Topic	Description
Details of the investigation:	Name and any tax identification number of the taxpayer under investigation, suspects, suspected offences, and investigation period. Suspects details shall include name, address and their national identity card number (or other identifying information).
Objectives of Investigation	In this section explain the why an investigation of taxpayer was instigated.
Summary of Investigation	Brief explanation on the investigation findings. Whether the suspected offence was committed and if so, were you able to gather enough evidence to prosecute the suspects.
Investigation Procedure	Detail procedure of how the investigation was conducted. Include works done in both pre investigation and during investigation stage.
Evidence Gathered and Observation	Details of evidence collected during the investigation process and their findings. All relevant law and all relevant evidence must be listed in the sections prior before the law is applied to the evidence and circumstances of the suspect.
Suspects and Reasons for suspect	For each suspect, suspected offence, offence period and reason for suspect, and evidence to support the suspected offence shall be explained separately.
Recommendation	Based on the finding above, what legal action is recommended to be taken – for example, forwarding the case for prosecution or closing the case (and potentially sending it back for assessment of outstanding taxes).
Investigation Team	Include names and designation of the investigation teams. This includes investigation officer, case officer(s) and supervisor.

26 Referral for prosecution

The decision on whether to progress a case to prosecution is arguably the most important part of the criminal process. Jurisdictions will typically have distinct legislation supported by prosecution guidelines or regulations that will govern the different stages of criminal prosecution. Where this is in place, the TCIM should clearly cross reference/link to this guidance as appropriate. However, this part of the TCIM should outline the roles and responsibilities of investigators and prosecutors at different stages of prosecution. While these will vary depending on the country's legal framework, some of the stages of prosecution that are common to many jurisdictions are outlined below.

Role of the prosecution authority at the investigative stage

The prosecution authority is the government agency that represents the state before the courts. Typically, countries adopt one of three models for prosecution of tax crimes (OECD, 2017[5]):

- **Central prosecution authority responsible for the investigation and prosecution of tax crimes**. Under this mode the prosecution will often delegate significant elements of the investigation to other agencies such as the Police or the tax administration.
- **Central prosecution authority with no responsibility for criminal tax investigations.** Under this model the prosecution authority does not participate in or direct the investigation. However, public prosecutors may advise agencies on the judicial process and laws of evidence throughout the investigation and will review the investigation file in collaboration with the investigation agency before the case is submitted for prosecution.
- **Law enforcement agencies may prosecute offences directly.** Under this model the agency responsible for investigating the tax crime (e.g. the tax administration) can also prosecute the offence

As outlined above, the extent to which public prosecutors are involved in tax crime investigations will vary between jurisdictions. For the most part, prosecutors tend to direct investigations in civil law jurisdictions, whereas in common law jurisdictions the investigating agency directs its own investigation before referring the case for prosecution. The TCIM should clearly state the model adopted in a jurisdiction, defining the roles and responsibilities of investigators and prosecutors during the investigation of the tax crime.

Referral for prosecution

The TCIM should outline in detail the process for referring a case for prosecution. In some jurisdictions this may be automatic (e.g. where the alleged offence serious in nature, involves money over a certain threshold, etc.). In other jurisdictions, investigators will need to make this assessment based on the quality and quantity of evidence obtained during the investigation.

Decision to charge

The decision to charge a person with a tax crime typically sits with the prosecution and generally relies on two key factors being met:

- The evidence is sufficient for there to be a reasonable chance of conviction;
- Prosecution is in the public interest.

Pre-trial proceedings

Following a suspect's arrest, there is an initial appearance in front of a judge where the defendant will be informed of the charges against them and typically be required to enter a plea of guilty or not guilty. In some jurisdictions there may be a preliminary hearing or grand jury to determine whether there is probable cause for the charges and an opportunity for either side to submit pre-trial motions. This is followed by the discovery process where evidence must be shared between the defence and prosecution and plea negotiations may take place. The TCIM should include:

- Clear guidelines about how the charges must be communicated to the defendant according to the specific legal framework operating in the jurisdiction.
- A list of potential procedural consequences of failing to communicate the charges correctly, and the rights at stake for the defendant when this happens.
- A description of the specific steps that the prosecution must take to ensure the plea entered by the defendant is valid.
- Information on how to comply with laws on discovery
- Information on the availability of settlements

Trial/Hearing

Depending on the jurisdiction, the trial/hearing will take place in front a judge-alone or a jury. Usually witnesses share evidence with the court, gathered and articulated at the investigative phase. Investigators and tax authorities may themselves be called as witnesses. Following a foundational criminal law principle, prosecutors must prove the case beyond reasonable doubt, which is why the robustness of the evidence collected in the initial stages of the process is key for success. This is underpinned by the principle according to which a person is innocent until proven otherwise. After all the evidence has been reviewed, either the judge or the jury will make a decision in relation to culpability. The defendant may be found guilty or some or all charges, or non-guilty. If the latter occurs, the defendant is acquitted. On the contrary, if the former occurs, a date is set for sentencing.

Against this backdrop, this section of the manual should include:

- Guidance and examples on what constitutes reasonable doubt in the context of a tax crime prosecution;
- Guidance for investigators and tax authorities to prepare them as a witness.

Sentencing

After a guilty verdict, it is typically up to a judge to determine the appropriate penalty, in line with the sanctions available in legislation and supporting sentencing guidelines. Penalties can take many forms, including imprisonment and/or punitive fines. In addition to traditional criminal sanctions, a judge may also impose a range of civil and/or administrative penalties. For example, reparations, debarment from public procurement projects, and/or business prohibition orders. In some jurisdictions, confiscation/forfeiture of the instruments and/or proceeds of crime can also be imposed as a punitive sanction upon conviction. In other jurisdictions (typically those with a non-conviction based asset recovery regime or hybrid thereof), assets may be confiscated without the need for a conviction (for example, where the law provides a civil standard of proof with respect the confiscation/forfeiture of assets linked to criminal conduct) (see section 17 on asset recovery).

The sanctions imposed in criminal tax matters will vary between jurisdictions and depend on the gravity of the tax crime committed. However, it should always be based upon the principle of proportionality. In the context of the right to due process, a defendant can appeal the judgement, contesting both the guilty verdict and the severity of the penalty imposed. Accordingly, this section of the manual should include:

- A description of how the principle of proportionality operates in relation to the penalty, specifically tailored to tax crimes.
- An explanation about how the type and length of the penalty is determined in that jurisdiction.
- A thorough description of the appeals process and the consequences it might have for the evidence already collected and presented.

Box 24. Successful prosecution of large scale tax fraud in Mexico

In 2013, a money laundering investigation led by the specialized unit of the then Office of the Attorney General (Procuraduría General de la República, PGR) uncovered strong evidence of tax fraud committed by a high-income taxpayer who had reported substantially lower income than was actually earned. The case was referred to the Federal Tax Prosecutor's Office (Procuraduría Fiscal de la Federación, PFF) of the Ministry of Finance (Secretaría de Hacienda y Crédito Público, SHCP), which confirmed the omission of taxable income exceeding USD 5.75 million, representing patrimonial damage to the State estimated at of approximately USD 1.73 million in unpaid income tax.

That same year, the PFF filed a formal criminal complaint with the PGR, and the case was brought before a federal judge. On November 26, 2013, an arrest warrant was issued and executed on the same day. This marked the beginning of a criminal proceeding that would later set a precedent in the prosecution of large-scale tax offenses in Mexico.

During the trial phase, multiple pieces of evidence were presented, including a specialized forensic accounting report prepared by the PGR's Anti-Money Laundering Investigation Unit. Once the evidence stage was concluded, the presiding judge issued a conviction, sentencing the defendant to three years in prison and ordering payment of restitution, which at that time amounted to approximately USD 3.23 million. The court also explicitly denied the substitution of imprisonment and the conditional suspension of the sentence, in recognition of the seriousness of the offense and the harm caused to public finances.

The defendant filed several legal remedies, including an appeal, constitutional trials (amparos), and a constitutional review of some articles of the Tax Code before the Supreme Court of Justice. These challenges argued the potential unconstitutionality of certain tax and financial provisions. However, in all instances, the conviction was consistently upheld by the federal courts and the Supreme Court of Justice, ultimately becoming final and fully enforceable.

Subsequently, the defendant requested to pay the restitution in installments and to delay his entry into prison during the payment period. The court approved a conditional payment scheme backed by a mortgage guarantee. The SHCP, through the PFF, actively participated to ensure that the arrangement did not undermine the effectiveness of the sentence or allow impunity.

Between 2020 and 2021, the defendant began making court-ordered payments, starting with 20% of the total restitution (approximately USD 645,000) and securing the remaining 80% (around USD 2.58 million) through a mortgage on a property in Mexico City. He then made monthly payments of approximately USD 215,000 in accordance with the court-imposed schedule. In 2022, the defendant completed full payment of the court-ordered amount, amounting approximately USD 3.23 million.

During the proceedings, the SHCP also formally objected to the granting of penitentiary benefits, such as sentence substitution or commutation, arguing that tax fraud should not be considered a minor offense—particularly not at this scale. Although the judge eventually granted a conditional sentence, the SHCP's firm position underscored the importance of maintaining effective consequences for serious tax crimes.

This case involved a tax fraud exceeding USD 5 million, making it highly relevant for the tax administration. The criminal proceedings led to a final conviction and the full recovery of public funds. As of today, the restitution has been fully paid, making this case a benchmark for institutional effectiveness in the criminal prosecution of tax offenses in Mexico.

Source: PFF, Mexico (2025).

27 Post investigation procedures

The TCIM should provide guidance to investigators on the procedures to follow once a case has been referred for prosecution, closed, or otherwise suspended. This should include guidance on the procedures to follow for, among others:

- Handling of physical and digital evidence (i.e. should typically remain in an evidence room/digital forensic laboratory until it is required in court).
- Appropriate filing of hard copies of documents.
- Release of documents to taxpayers (e.g. where a copy or photograph is sufficient for record keeping purposes).
- Return of seized items to taxpayers.
- Disposal or uncollected documents or it.

References

Betti, S., V. Kozin and J. Brun (2021), *Order without Border: Direct Enforcement of Foreign Restraint and Confiscation Decisions, International Development in Focus*, World Bank, http://hdl.handle.net/10986/36691. [22]

Bostwick, L. et al. (2023), *Managing Seized and Confiscated Assets - A Guide for Practitioners*, World Bank, http://hdl.handle.net/10986/40920". [16]

Cebreiro Gomez, A. et al. (2022), *Taxing Crime: A Whole-of-Government Approach to Fighting Corruption, Money Laundering, and Tax Crimes*, http://hdl.handle.net/10986/37608. [14]

CiFAR (2022), *Civil Society Organisations & Asset Recovery - A Manual for Action*, https://cifar.eu/wp-content/uploads/2022/07/CSOs-and-asset-recovery-a-manual-for-action.pdf. [21]

Council of Europe (2023), *Guidelines for the Management of Seized Assets*, https://rm.coe.int/prems-015223-gbr-2204-guidelines-for-the-management-of-seized-assets-w/1680ad3f1a. [18]

FATF (2023), *Recovering International Proceeds of Crime through Inter-Agency Networks*, FATF, Paris, https://www.fatf-gafi.org/en/publications/Methodsandtrends/recovering-international-proceeds-crime-inter-agency-networks.html. [19]

FATF (2012), *Best Practices on Confiscation (Recommendations 4 and 39) and a Framework for ongoing Work on Asset Recovery*, FATF, Paris, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Bestpracticesonconfiscationrecommendations4and38andaframeworkforongoingworkonassetrecovery.html. [20]

FATF (2012-2025), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html. [7]

Internal Revenue Service (2023), *Internal Revenue Manual*, https://www.irs.gov/irm. [2]

INTERPOL (2019), *Global guidelines for digital forensics laboratories*, https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf. [15]

Kenya Revenue Authorithy, I. (2019), *Tax Investigations Handbook. Taxpayer Edition.*, https://www.kra.go.ke/images/publications/KRA-TAX-INVESTIGATION-FRAMEWORK-1.pdf. [3]

OECD (2024), *Bringing Tax Transparency to Crypto Assets - An Update: Global Forum Report to G20 Finance Ministers and Central Bank Governors*, OECD Publishing, https://doi.org/10.1787/b33c9aa1-en. [8]

OECD (2024), *Designing a National Strategy against Tax Crime: Core Elements and Considerations*, OECD Publishing, Paris, https://doi.org/10.1787/0e451c90-en. [4]

OECD (2023), *Enhancing Inter-Agency Trust Between Tax and Other Financial Crime Authorities: Pilot Inter-Agency Trust Maturity Model and Trust Perception Survey*, OECD, Paris, https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-and-crime/pilot-inter-agency-trust-maturity-model-and-trust-perception-survey.pdf. [9]

OECD (2022), *Recommendation of the Council on the Ten Global Principles for Fighting Tax Crime*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0469. [1]

OECD (2021), *Fighting Tax Crime – The Ten Global Principles, Second Edition*, OECD Publishing, Paris, https://doi.org/10.1787/006a6512-en. [6]

OECD (2020), *Tax Crime Investigation Maturity Model*, OECD, Paris, https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-and-crime/tax-crime-investigation-maturity-model.pdf. [13]

OECD (2018), *Improving Co-operation between Tax Authorities and Anti-Corruption Authorities in Combating Tax Crime and Corruption*, OECD Publishing, Paris, https://doi.org/10.1787/c8c44bcf-en. [11]

OECD (2017), *Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes - Third Edition*, OECD Publishing, Paris, https://doi.org/10.1787/af874d4a-en. [5]

OECD (2013), *Bribery and Corruption Awareness Handbook for Tax Examiners and Tax Auditors*, OECD Publishing, https://doi.org/10.1787/9789264205376-en. [10]

OECD (2009), *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, OECD, Paris, https://www.oecd.org/en/publications/money-laundering-awareness-handbook-for-tax-examiners-and-tax-auditors_9789264081093-en.html. [12]

Secretariat to the UNCAC Conference of State Parties. (2018), *Revised draft non-binding guidelines on the management of*, https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/ImplementationReviewGroup/12-14November2018/V1807476e.pdf. [23]

Sotiropoulou, A. et al. (2021), *Asset Recovery Handbook: A Guide for Practitioners, Second Edition, StAR Initiative*, World Bank, http://hdl.handle.net/10986/34843. [25]

United Nations (1948), *The Universal Declaration of Human Rights*, https://www.un.org/en/about-us/universal-declaration-of-human-rights (accessed on 22 January 2025). [26]

UNODC (2017), *Effective management and disposal of seized and confiscated assets*, https://www.unodc.org/documents/corruption/Publications/2017/17-07000_ebook_sr.pdf. [24]

UNODC (2004), *United Nations Convention Against Transnational Organized Crime and The Protocols Thereto*, https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf. [17]

Designing a tax crime investigation manual

Key elements and considerations

Tax crimes have a detrimental impact on all countries, hindering domestic resource mobilisation and eroding public confidence in government and financial systems. This can result in wide-ranging negative outcomes, as resources are diverted away from critical public services and infrastructure, and in many cases, used to finance other serious crimes such as corruption, the trafficking of goods and people, and terrorism. Combatting tax crimes requires a swift and co-ordinated response from tax and other financial crime authorities, governed by clear and transparent laws and processes. This guidance tool is designed to encourage and support governments in the development of domestic manuals to guide law enforcement authorities through each stage of a criminal tax investigation. Adherence to legal and operational procedures is critical to any successful enforcement action and jurisdictions are encouraged to use this guide to enhance the effectiveness, efficiency, and integrity of their tax crime investigations whilst ensuring that suspects' rights are upheld at all times.