Designing a National Strategy against Tax Crime

CORE ELEMENTS AND CONSIDERATIONS

OECD

Designing a National Strategy against Tax Crime

CORE ELEMENTS AND CONSIDERATIONS

OECD
BETTER POLICIES FOR BETTER LIVES

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

ISBN 978-92-64-60508-4 (PDF)

Photo credits: Cover © CoreDESIGN/Shutterstock.com.

Corrigenda to OECD publications may be found on line at: www.oecd.org/about/publishing/corrigenda.htm.

© OECD 2024

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at https://www.oecd.org/termsandconditions.

Preface

The financial world is ever-changing. The speed and means with which money moves in today's world was unfathomable thirty years ago. While most taxpayers are honest and pay their taxes, even the slightest increase in a country's tax gap can threaten national security. A comprehensive national tax crime strategy is imperative not only to ensure that countries collect what is due, but also to provide a foundation for the tax system based on confidence in government and consequences for those who evade their responsibilities. Combatting tax and other financial crimes is paramount to maintaining the integrity of our economic systems, and the release of this report is a significant milestone in ongoing efforts to address illicit activities and uphold the rule of law.

National tax crime strategies differ from country to country, but arguably the most important part of any strategy is the need for each country to conduct their own risk assessment to identify vulnerabilities and potential areas of exploitation. By understanding the evolving landscape of tax crimes, we can proactively implement measures to prevent, detect, and deter illicit activities that undermine the fairness and effectiveness of our tax systems.

This paper also includes suggestions on how to enhance information sharing, capacity building and collaboration among tax authorities and law enforcement agencies. By strengthening our collective response to tax crimes, we can better protect our economies from the harmful effects of tax evasion, tax fraud and money laundering. Furthermore, through ongoing monitoring and feedback mechanisms, we can adapt and refine our approach to stay ahead of evolving tax crime trends and safeguard the integrity of our tax systems.

I challenge you to read this report with an eye for something that can make your country better. Challenge the status quo and make tough decisions. As we all embark on this journey to combat tax crimes and promote compliance, I call upon tax crime agencies, law enforcement and international partners to join us in this critical endeavour. Together, we can build a more resilient and transparent tax environment that upholds the principles of accountability, fairness, and justice for all.

Finally, I would like to extend my gratitude to colleagues from the Task Force on Tax Crime and Other Crimes (TFTC) Secretariat and IRS Criminal Investigation for their work in writing this report, and to TFTC members for their excellent contributions.

Daniel Werfel

Commissioner, Internal Revenue Service

Foreword

This report seeks to support Principle Two of OECD Council Recommendation on the Ten Global Principles for Fighting Tax Crime which recommends that jurisdictions devise an effective strategy for addressing tax crimes and related crimes, including through processes to identify the key risks and through engagement with other agencies and relevant stakeholders. The report sets out suggested core elements of a strategy for jurisdictions to consider and provides a number of country examples which jurisdictions may want to draw on for inspiration.

The report was drafted by Fiona May and Marcos Roca of the OECD Secretariat, under the supervision of Peter Green, with the support of officials of the United States Internal Revenue Service Criminal Investigation. The authors would also like to thank all members of the OECD Task Force on Tax Crimes and Other Crimes for their input and the many country examples that were provided to enrich the 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

Abbreviations and acronyms 7

Executive Summary 10

1 Introduction 12
- Who has responsibility for the national tax crime strategy? 12
- Why develop a national tax crime strategy? 14

2 Conducting a Tax Crime Risk Assessment 19
- Key concepts and terms relevant to the TCRA 20
- Participants in the TCRA framework 21
- Preparing a TCRA 22
- Evaluation of the risks identified in the TCRA 30

3 Developing the Strategy 36
- Defining the objectives and goals of the tax crime strategy 37
- Developing an operational plan 37
- Available Resources 40
- Domestic Stakeholder Collaboration: A whole of government approach 43
- International Co-operation: Identification of key cross-border stakeholders 47
- Preparing a communications strategy 48

4 Monitoring, Evaluation, and Impact Measurement 54
- Identification of indicators 55
- Value for Money 57

5 Case studies 59
- A Case Study from the Internal Revenue Service - Chile 59
- A Case Study from the Internal Revenue Service – Criminal Investigations – United States 61
- A case study from His Majesty's Revenue & Customs – United Kingdom 68

References 71

FIGURES

Figure 1.1. Role of administration in tax crime investigations (2021) 13
Figure 1.2. Potential consequences of tax crime 15
Figure 2.1. Overview of the TCRA 26
Figure 2.2. Risk matrix 31
Figure 3.1. Possible elements of a tax crime strategy 36
Figure 3.2. Core elements for addressing identified risks 37
Figure 3.3. Available Resources 40
Figure 3.4. Investigation and enforcement tools 42
Figure 3.5. Key actors to involve in a whole of government tax crime strategy 44
Figure 3.6. Stakeholder engagement: A suggested guide 45
Figure 3.7. Communicating the strategy 50
Figure 4.1. Process for measuring the effectiveness of the strategy 55
Figure 4.2. Potential categories of indicators 55

Abbreviations and acronyms

3PML	Third Party Money Laundering
ABF	Australian Border Force
AFP	Australian Federal Police
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
ATO	Australian Taxation Office
BOD	Business Operating Division
BSA	Bank Secrecy Act
CCO	Corporate Criminal Offence
CDPP	Commonwealth Director of Public Prosecutions
CRA	Canada Revenue Agency
DGT	Directorate General of Taxes
DIAN	National Tax and Customs Administration of Colombia
DOJ	Department of Justice
EPPO	European Public Prosecutor's Office
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
HIDTA	High Intensity Drug Trafficking Area
HMRC	HM Revenue and Customs
HVT	High-Value Target

IDT	Identity Theft
IFF	Illicit Financial Flows
IRS	Internal Revenue Service
IRS-CI	Internal Revenue Service - Criminal Investigation
J5	Joint Chiefs of Global Tax Enforcement
LSR	Leadership Succession Review
MIGCT	Integrated Tax Compliance Management Model
MoU	Memorandum of Understanding
NCIU	Nationally Coordinated Investigations Unit
NGO	Non-Governmental Organisation
OCDETF	Organised Crime Drug Enforcement Task Forces
OECD	Organisation for Economic Co-operation and Development
PGCT	Tax Compliance Management Plan
PIF	Protection of the financial interests of the European Union.
POLFA	Fiscal and Customs. Police Force of Colombia
QRP	Questionable Refund Programme
ROI	Return on Investment
RPP	Return Preparer Programme
SDGs	Sustainable Development Goals
SFCT	Serious Financial Crime Taskforce
SII	Chilean Revenue Service
SIRF	Stolen Identity Refund Fraud
SOCTA	Serious and Organised Crime Threat Assessments
STA	Sweden Tax Authority
TAS	Tax Administration Series
TBML	Trade Based Money Laundering

TCRA	Tax Crime Risk Assessment
TEOAF	Treasury Executive Office for Asset Forfeiture
TFTC	Task Force on Tax Crimes and other Crimes
TOC	Transnational Organised Crime
ToR	Terms of Reference
UAF	Financial Analysis Unit
UNODC	United Nations Office on Drugs and Crime
VASPs	Virtual Asset Service Providers
VAT/GST	Value Added Tax/ Goods and Services Tax

Executive Summary

Most taxpayers are law-abiding and comply voluntarily with their tax obligations, supported by tax administrations through the provision of guidance, bespoke assistance, and the increasing use of digital taxpayer services, such as electronic filing and payments and the pre-filling of tax returns. There is however a small subset of individuals, companies and entities, as well as organised criminal groups, that take deliberate steps not to comply with their tax obligations or who commit other forms of tax crime, for example fraudulently claiming refunds.

Tax crimes negatively affect all countries, developed and developing alike. They obstruct governments' ability to collect revenue and undermine trust in the legal and financial system which can lead to a wide range of adverse outcomes. Tax crime is often closely linked to other forms of serious domestic and transnational crime, such as money laundering, the trafficking of drugs or people, and terrorist financing.

This report sets out the rationale for adopting a national strategy for countering tax crime and to support jurisdictions' efforts in designing such strategies, drawing from the practices of members of the OECD's Task Force on Tax Crimes and other Crimes (TFTC).

As with tax compliance in general, it is not possible to conduct investigations for all potential breaches of tax law and a risk-based approach must be adopted. An effective strategy will therefore focus on the main risks, both existing and emerging, set clear objectives and priorities, and be subject to periodic monitoring and evaluation.

This report is divided into five chapters:

- **Chapter 1. Introduction.** This briefly sets out the potential impacts of tax crime and the rationale for the development of a national tax crime strategy.
- **Chapter 2. Conducting a tax crime risk assessment.** This highlights the importance of understanding risks, which will include threats and vulnerabilities, as part of developing or reviewing a national tax crime strategy. It also stresses the importance of using a wide range of sources of information and input from other stakeholders, both in the public and private sector. This will help authorities mandated to prevent and investigate tax crime ensure that their strategy is focussed on responding effectively to the main priorities, that resources are used most effectively, including taking account of the role of other stakeholders, and also allow for the development of well-argued business cases for additional resource where necessary.
- **Chapter 0. Core elements of developing a national tax crime strategy.** This chapter sets out guidance for the development of the strategy itself, based on the results of the tax crime risk assessment, including the establishment of measurable objectives, prioritisation of risks, the identification of key actions and the communication of the strategy internally and externally.
- [1]**Chapter 4. Monitoring and evaluation.** This looks at how the strategy can be effectively monitored and evaluated, to ensure that it can be updated where appropriate to take account both of the evolution of tax crime as well as the availability of new tools, practices, and policies for countering such crimes.
- **Chapter 5. Case studies.** This final chapter sets out three short case studies on the development of national tax crime strategies from Chile, the United States and the United Kingdom. These are

high-level overviews and are intended to provide food-for-thought for other jurisdictions seeking to develop or review their national tax crime strategy.

Caveat

Tax crime enforcement agencies operate in varied environments, and the way in which they each administer their work differs in respect to their policy context, legislative environment, and administrative practice and culture. As a result, due regard needs to be paid to the distinct challenges and priorities each agency and jurisdiction is managing and a standard approach to tax crime strategies may be neither practical nor desirable. This report is therefore intended to assist administrations in their domestic considerations regarding the development and implementation of an efficient and effective strategy against tax crime.

1 Introduction

The aim of this report is to support jurisdictions seeking to implement Principle 2 of the OECD Recommendation of the Council on the Ten Global Principles for Fighting Tax Crime (hereafter, "the Recommendation") (OECD, 2022[1]). Principle 2 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.

As set out in the Recommendation, 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. 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 be relevant both to a tax crime risk assessment (TCRA) and a tax crime strategy given that there are often strong interlinkages.

While the Recommendation does not distinguish between different types of tax crime, this is a core consideration in the development of tax crime strategies where it may be desirable to take different approaches to different types of tax crime, in particular, regarding choices of whether to take civil or criminal action in particular cases.

The Recommendation also underscores that more than one government agency may be mandated to detect, investigate, prosecute, and/or recover the proceeds of tax crimes, which will need to be reflected in tax crime strategies. The exact type, layout, and powers of each agency will vary depending on the country. In some jurisdictions there may be a single agency, such as the tax administration, while in others the mandate may be spread across several different agencies (e.g. police, prosecution service, specialised financial crime agencies etc.)

Who has responsibility for the national tax crime strategy?

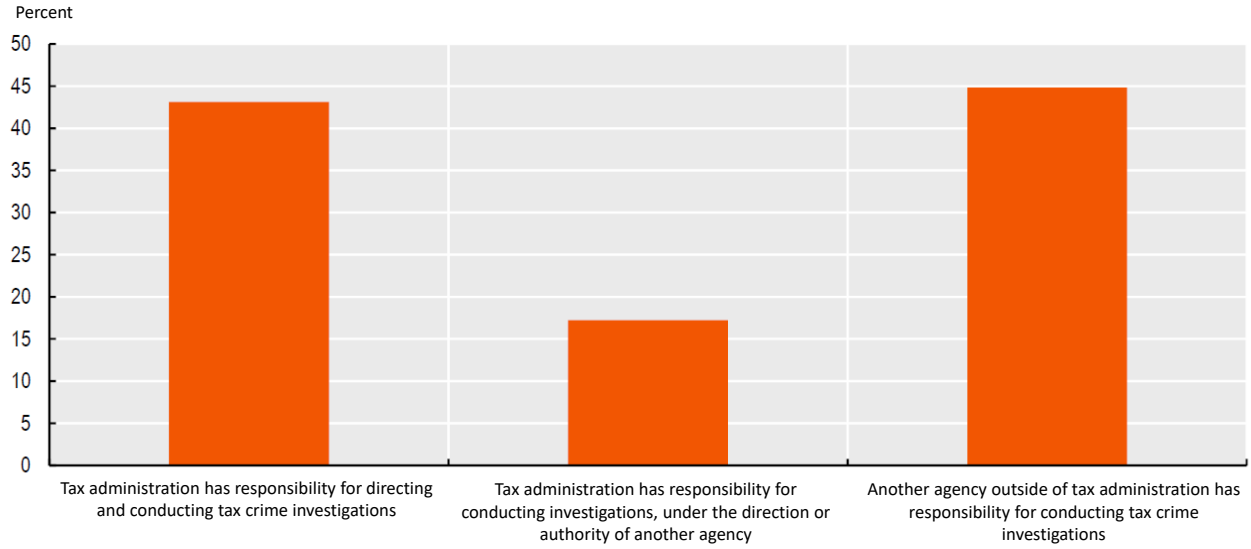
Which agency has responsibility for the strategy depends on whether the tax crime enforcement agency sits in the tax administration; is a stand-alone agency; or is split across multiple agencies. There is no right or wrong approach, and it will depend on the organisational structure in a particular jurisdiction as well as the legal system, policy context, legislative environment and general structure of law enforcement.

Of the 58 tax administrations surveyed for the OECD Tax Administration Series (TAS), close to 45% have responsibility for directing and conducting tax crime investigations (OECD, 2023[2]).

In the remaining jurisdictions surveyed, tax administrations only have responsibility for conducting investigations under the direction or authority of another agency, or tax crime investigations are completely the responsibility of other agencies, for example the police or public prosecutor or a specialist tax or financial agency, established outside the tax administration (see Figure 1.1)

Figure 1.1. Role of administration in tax crime investigations (2021)

Percent of administrations



Note: In some jurisdictions, the organisational approach for tax crime investigations may depend on the tax offence or tax-related criminal proceedings. In those cases, an administration may be selected multiple answer options. This is why the percentages add up to more than 100%.
Source: Tax Administration Series 2023, table A.69

The key issue for jurisdictions to consider, though, is how to achieve an effective and efficient tax crime strategy taking account of the responsibilities and powers of the different agencies mandated to fight tax and other financial crime. For example, in many cases the primary responsibility for tackling tax crime will lie with a particular function within the tax administration. In that case, how tax crime is addressed, for example which tools and powers should be used in different cases, may be looked at as part of an administration wide tax compliance strategy. Nevertheless, it will be important that the impacts and specificities of tax crime are looked at in their own right for the reasons set out below regarding the rationale for a tax crime strategy. If this was not the case, it would not be clear how individual cases should be dealt with, and what role and resources should be assigned to the tax crime investigation function.

For this reason and for the sake of simplicity, in the rest of this report, it is assumed that the strategy is developed by the body or function with primary responsibility for tax crime investigation. That is referred to as the tax crime enforcement agency in this report, although it should be understood that this could equally be a tax crime investigation unit or division within the tax administration and “tax crime enforcement agency” should be read with that in mind.

Given each jurisdiction is likely to have multiple agencies with functions relevant to the fight against tax crime, there will be a continuing emphasis in this report on the value of a whole of government strategy taking full account of the roles of various agencies who have a responsibility for tackling tax crime so as not to leave gaps or create inconsistencies of approach (for example regarding the use of civil or criminal powers).

Why develop a national tax crime strategy?

The importance of developing a national crime strategy comes from three main underlying factors which, if not considered within a strategy, may give rise to practical difficulties in tackling tax crime efficiently and effectively as well as potentially leaving gaps that criminals can exploit. These factors are that:

- tax crime can have serious and wide-ranging consequences beyond direct revenue losses;
- there will always be limited resources for tackling tax crime which means that decisions on prioritisation are required; and
- there are multiple actors and tools.

Tax crime can have serious consequences

Tax crimes can range in scale and scope, from tax evasion or refund fraud committed by individuals or businesses to larger scale crimes which may be carried out by organised criminal groups, including across borders.

The loss of tax revenue and the consequent impact on a government's ability to fund public services is the obvious immediate consequence of tax crime. Large scale, organised, fraud has perhaps the most visible impact, for example Europol estimates that organised VAT carousel fraud costs European Member States approximately €50 billion annually[1]. However, the impacts of tax evasion committed by significant numbers of individuals and businesses, when looked at across the economy as a whole, can also have highly damaging impacts. For example, and to give a sense of scale, in the area of offshore tax evasion, the OECD's Global Forum on Tax Transparency and Exchange of Information for Tax Purposes estimates that voluntary disclosure programmes, offshore tax investigations and related measures have helped identify close to EUR 126 billion in additional revenues.[2]

However, as set out in Figure 1.2, tax crime has many other less visible but highly damaging consequences. For example:

- Within a particular sector, tax evasion undertaken by dishonest businesses or those operating in the shadow economy can have significant impacts on honest businesses which may struggle to compete;
- If tax crime is perceived as prevalent within a sector or within a jurisdiction more generally, it can undermine confidence in the fairness of the tax system and potentially lead to lower voluntary compliance over time. It can also lead to reduced business investments, including foreign direct investment, or the application of controls on the flow of funds to particular jurisdictions;
- The proceeds of tax crime, particularly organised tax crime, can be used to fund other serious crimes and lead to a growth in illicit financial flows across borders. The United Nations Office on Drugs and Crime estimate criminal proceeds from all illicit activities represent around 3.6% of global GDP or USD 2.1 trillion (United Nations Office on Drugs and Crime, 2011[3]);
- Tax crime can increasingly be carried out remotely, meaning that unchecked tax crime in one jurisdiction can impact revenues in another jurisdiction as well as individual taxpayers through tax scams;
- The effort and cost of tackling tax crime can reduce the resources available to the tax administration to modernise and enhance services which would otherwise reduce burdens on honest taxpayers and support voluntary compliance.

Figure 1.2. Potential consequences of tax crime

Source: OECD 2024

Keeping a focus on priority areas

In a world of limited resources, tax crime enforcement agencies cannot investigate every potential case of tax crime. Prioritisation is therefore needed, and a strategy will allow that prioritisation to be set out clearly, making it easier for decision-makers both when deciding on resource allocation as well as the appropriate actions in individual cases.

While a primary focus may often be investigating, sanctioning, and recovering revenue losses from larger scale criminal activity, it is likely to lead to better outcomes over time if jurisdictions also consider the other impacts of tax crime outlined above when setting out their priorities. A wider cost-benefit calculation, which also looks over the medium term, can also result in the prioritisation of actions aimed at changing future behaviours and enhancing public confidence as well as tackling more serious crimes. This may lead at various times to more efforts being put into investigating cases of tax crime where there may be a relatively small revenue loss that has occurred in order to change behaviour more widely and thus protect larger amounts of revenue. Examples of this might be criminal investigations of individuals or businesses in particular sectors where tax crime may be more prevalent.

Tax crime can potentially be tackled in multiple ways

A strategy can help ensure that tax crime is tackled as effectively and efficiently as possible, using all available tools and actors, as well as the consideration of how best to close gaps. Unpacking this further, a strategy can:

Help determine when to use civil versus criminal powers

In most jurisdictions, it is possible to investigate and sanction tax crimes, as well as recover revenue, through the use of civil powers. This can often result in revenue being recovered more quickly and lead to lower costs for the administration than investigating, prosecuting, and recovering using criminal powers. However, if all cases were resolved through the use of civil powers, this may affect taxpayer behaviours over time, since the impact of civil cases on individuals and businesses are often less than the impact of a successful criminal prosecution. A balance therefore needs to be struck between the use of civil and criminal powers.

A strategy can be helpful in guiding these decisions by setting out general criteria as to when cases should be dealt with through civil or criminal powers. This might cover:

- The seriousness of the tax crime in terms of its scale or impact on public confidence;
- The costs involved in criminal processes compared to the costs involved in civil processes;
- The likelihood of success in a criminal case given the higher burden of proof;
- The extent to which civil processes have a wider deterrence effect both on the particular individual or business, or more widely (This might depend on factors in a particular jurisdiction such as the level and types of penalties, publicity of the sanction, future auditing that might result etc.);
- The impacts on revenue and other consequences of tax crime over the medium term if the risks of prosecution for tax crime is seen as very low;
- Whether the tax crime is carried out by organised criminal groups who will continue to engage in tax crime;
- Connections with other serious crimes, such as money-laundering, bribery and corruption, or drugs trade.

Supports a whole-of-government approach to combatting financial crime

As noted, in many jurisdictions, tax crimes are the responsibility of more than one agency. Even where that is not the case, tax crimes are often committed by criminals being investigated for other illegal activity, such as money laundering or bribery and corruption. In addition, criminal tax behaviour may be linked to investigation into breaches of rules applying to regulated activities, such as financial and professional services.

Identifying all stakeholders who might have information about potential tax crimes or who should be told about suspicions of other criminal activity is critical to informing decisions about which agency or agencies are best placed to investigate, prosecute and recover proceeds in particular cases. This may lead, in some cases, to the integration, or partial integration, of the tax crime strategy into a wider national crime strategy where some or all of the agencies agree to share information and co-operate in a whole-of-government approach. This is reflected in Principle 8 of the Ten Global Principles, which recommends that jurisdictions:

Establish effective legal, administrative, institutional, and operational frameworks for domestic inter-agency co-operation, including:

a) reporting and information sharing by tax authorities of suspicions of tax crimes and other financial crimes, including corruption, money laundering and terrorism financing, arising out of the

performance of their duties, to the appropriate domestic law enforcement authorities and, where applicable, to the Financial Intelligence Units;

b) *reporting and information sharing between all appropriate domestic authorities, including law enforcement authorities, with respect to the enforcement of tax crimes and other financial crimes within their respective mandates; and*

c) *mechanisms to support enhanced forms of co-operation among tax authorities, competent authorities, and other appropriate domestic law enforcement authorities responsible for enforcing financial crimes, such as joint operations and taskforces.*

In addition, reflecting Principle 9 of the Ten Global Principles, jurisdictions may want to reference co-operation with tax crime enforcement agencies in other jurisdictions in their strategy, whether there are current arrangements in place or there is a desire to establish them. Tax crimes can increasingly happen across borders, often in real-time and enabled by new technologies, including cryptocurrencies. Without effective international co-operation it can be impossible in some cases to progress tax crime investigations or recover the proceeds of crime. Taking a strategic view to such partnerships, based on the tax crime risk analysis, is likely to become an increasingly important feature of national tax crime strategies.

Box 1.1. A whole-of-government approach to tacking tax and other financial crime

In July 2015, the Serious Financial Crime Taskforce (SFCT) was established by the Australian Taxation Office (ATO) to help tackle the most serious forms of financial crime. The SFCT is a joint-agency taskforce established on 1 July 2015.

The Australian community loses millions of dollars of revenue each year as a consequence of serious financial crime. SFCT's mission is to prevent, detect, and deal with financial criminal activities together with partner agencies. By using the knowledge, resources, and experience of domestic law enforcement and regulatory agencies, the SFCT identifies and addresses the most urgent forms of financial crime in Australia. The Taskforce is focussed on combatting activities like offshore tax evasion, cybercrimes affecting the tax and superannuation systems, and illegal phoenix activity, among other types of financial crime.

Participating members of the SFCT include: ATO, Australian Federal Police (AFP), Australian Criminal Intelligence Commission, Attorney-General's Department Australian Transaction Reports and Analysis Centre, Australian Securities and Investments Commission, Commonwealth Director of Public Prosecutions (CDPP), Department of Home Affairs, incorporating its operational arm, the Australian Border Force (ABF) and Services Australia.

The Australian Government provided the SFCT with AUD 127.6 million for the period 2016-2020, and in December 2018, the ATO received additional AUD 182 million over four years to extend the SFCT. As of December 2023, the SFCT had raised liabilities of AUD 2.026 billion and collected over AUD 812 million. Furthermore, 1,994 audits had been completed and 33 people had been convicted and sentenced.

Source: Australian Taxation Office, 2024

Enhance system integrity

In addition to investigating and taking appropriate enforcement activity against tax crime, tax crime enforcement agencies will often be well placed to identify weaknesses in the current system that are being, or are capable of being, exploited by criminals.[3] Addressing these weaknesses may prevent many crimes or make them much more difficult. These may be, among other things:

- Loopholes in tax law or in the design of policies which criminals might seek to exploit, for example as has been seen in some countries with dividend stripping (OECD, 2023[4]);
- The ability of criminals to use cryptocurrencies and opaque legal structures to hide their identities;
- A lack of information to risk assess for tax crime, for example where there are few electronic data sources;
- The use of technology to remove information and allow underreporting or overclaiming of expenses, for example the use of software to create fake invoices or to remove payment information (OECD, 2017[5]);
- Weaknesses in identity or verification systems which may make identity fraud easier to commit, enabling refund fraud or other forms of tax crime;
- Systems that are vulnerable to cyber-attack.

While the responsibility for addressing these weaknesses may lie with other government authorities, for example policy makers, tax administrations, and/or other agencies, the tax crime enforcement agency can play an important role in identifying these weaknesses and calculating their seriousness, and make appropriate recommendations, including whether additional powers may be needed. In addition, it may make sense for tax crime enforcement agencies to be consulted on the design and implementation of new systems or policies, including regarding the digital transformation of tax administration as envisaged in Tax Administration 3.0 (OECD, 2020[6]). Referencing this role in a strategy can help to ensure that this potential role of the tax crime enforcement agency is understood and utilised where appropriate.

Notes

[1] See Operation Admiral: EPPO uncovers organised crime groups responsible for VAT fraud estimated at €2.2 billion, European Public Prosecutor's Office (https://www.eppo.europa.eu/en/news/operation-admiral-eppo-uncovers-organised-crime-groups-responsible-vat-fraud-estimated-eu22)

[2] Global Forum on Transparency and Exchange of Information for Tax Purposes – OECD - https://www.oecd.org/tax/transparency/

[3] Tax crime enforcement includes both investigations and prosecutions.

2 Conducting a Tax Crime Risk Assessment

Identifying, assessing, and understanding tax crime risks is an essential precursor to the implementation and development of a national tax crime strategy. A thorough risk assessment will detect external threats and existing vulnerabilities in, for instance, the legal framework, enforcement, and other areas. The results of a tax crime risk assessment can also provide useful information to other law enforcement and intelligence agencies when conducting their own risk assessments.

The implementation of a tax crime risk assessment framework and the delivery of a tax crime risk assessment (hereafter, the "TCRA") will provide both policymakers and investigators with a better and broader understanding of the challenges posed, the modus operandi used by tax criminals, and emerging trends. As tax crime is one of the most common predicate offences for other forms of serious crime, the TCRA will also serve in some cases as a precursor for broader serious crime risk assessments already in place, including but not limited to the National AML/CFT Risk Assessment referred to by FATF Recommendation 1 (FATF, 2012-2023[7]).

As with a national tax crime strategy, the TCRA may be conducted as an independent risk assessment or as part of a broader tax risk assessment. If conducted as a separate initiative, relevant (non-criminal) tax intelligence, including increased-risk areas that were detected by the civil tax authority, will feed into the TCRA.

Key concepts and terms relevant to the TCRA

Before discussing the elements of a TCRA, it is important to have a collective understanding of the terms that will be used throughout this document. Many of them come from the areas of risk management and risk assessment, which are common to both public and private sectors, while others are drawn from existing documents pertaining to assessing risks in the field of serious crime, such as FATF and UNODC guidance[1], and the area of civil/administrative tax risk management.

Broadly speaking, risk assessment is a process based on an agreed methodology that identifies, analyses, and understands risks related to tax crime, and serves as the first step in developing a strategy for responding to those risks.

In the current context of conducting a TCRA, this document assumes the following definitions, reflecting FATF guidance for AML/CFT risk assessments:

- ***Risk*** may be considered as a function of three factors:
  - ***Threat*****:** In the tax crime context, a threat is an individual, a legal person, an object, or an activity with the potential to cause harm to the economy, the state, society, or the tax base. This includes criminals, their enablers or facilitators, their funds, and assets, as well as past, present, and future criminal activity.
  - ***Vulnerability:*** Vulnerabilities may be exploited by the threat to support and facilitate criminal activities. In the tax crime context, vulnerabilities differ from threats in the fact that they are internal flaws, such as weaknesses in the enforcement system (legal or operational), or features of a particular sector, regulation or product type that make them appealing for tax crime purposes. A vulnerability can also be something, such as the introduction of a new system or policy, that has not been adequately assessed for its robustness against criminal attacks.
  - ***Consequence*****:** This refers to the impact or harm that a risk may cause. It includes the effect of underlying financial criminal activity on the tax base, government, the financial system, and society more generally. The consequences of tax crime may apply in the short, medium, or long term, and can relate to specific communities, business sectors or geographical locations, the general business environment, a jurisdictions' investment attractivity, and the overall international reputation of a country. In the financial crime context, incorporating consequences into the risk assessment framework may not require very sophisticated approaches (FATF, 2013[8]). Rather than trying to quantify consequences in monetary terms, jurisdictions may wish to focus on achieving a broad understanding of their threats and vulnerabilities and distinguish the scale and scope of different risks to inform the tax crime strategy.

Box 2.1. Tax crime and proceeds risk assessment

Example from the World Bank

The World Bank developed a methodology to support countries in assessing their risks of tax evasion and money laundering, focusing on the assessment of threats and vulnerabilities, following recommendation 1 of the Financial Action Task Force, and in line with Principle 2 of the Ten Global Principles. This stand-alone module is part of a broader tool developed by the World Bank to support countries assess their risk of money laundering.

The module on risk assessment of tax evasion and money laundering is divided into two submodules:

a) **Threats.** The first submodule seeks to assess the threat of tax crimes, therefore analysing external factors, such as the scale, incidence and size and nature of the proceeds of tax crimes, and common typologies, as well as related money laundering.
b) **Vulnerabilities**. The second submodule aims to assess anti-tax evasion mechanisms (legal, institutional, and operational good practices) and those internal factors that may enable tax evasion. The tool analyses vulnerabilities along three areas: (i) core tax obligations (registration, accurate record keeping, filing, correct reporting, and payment), (ii) falsehood and obstruction tax practices, (iii) specific tax evasion schemes (transfer pricing area, fraudulent schemes, and offshore schemes). In addition, the assessment focuses on five types of taxes: personal income tax, corporate income tax, payroll tax, consumption taxes (VAT/GST), and withholding taxes.

This self-assessment exercise requires a collaborative, multi-stakeholder process that promotes and protects trust, transparency, and inclusiveness, therefore supporting a whole of government approach. The module was designed to assist countries in building long term capacity and establish a process for regularly updating their understanding of the country's risks, and to support authorities to develop a national tax crime strategy.

Source:https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use

Participants in the TCRA framework

The TCRA will ideally be used by all government stakeholders involved in the fight against tax crime to assist them in formulating or updating their individual strategies and approaches to tackle tax crime. This includes, among others, policymakers, supervisors, operational agencies, and investigators. Subject to each jurisdictions' disclosure rules, some of the findings may also be shared with the private sector, especially with financial entities and with professional bodies that regulate professions where higher tax crime risks are identified, to conduct their own mitigation programmes. The number and type of agencies and users will vary according to the institutional framework of a jurisdiction, but some typical primary participants in the elaboration and use of the TCRA include:

- **Policymakers and operational staff of competent authorities involved in preventing, detecting, and prosecuting tax crime**. This may include a jurisdiction's tax crime enforcement agency, its tax administration, other law enforcement agencies where applicable, the asset forfeiture or asset recovery office, and the government service in charge of tax crime prosecutions.

- **Competent authorities involved in the fight against other financial crime**. This includes agencies such as the financial intelligence unit, customs, border control services, intelligence services, anti-corruption authorities, etc.
- **Market regulators**. This includes central banks, securities control authorities, financial services regulators, sectoral regulators etc. In some jurisdictions, company registries may also possess valuable information regarding the different legal vehicles employed by criminals.
- **Other agencies with relevant information.** In some jurisdictions, other authorities may also hold information that could be valuable when conducting the TCRA. For instance, agencies holding beneficial ownership information, statistics agencies which might provide estimates on the size and composition of the shadow economy and the agencies responsible for welfare or business developments which may have data pertaining to fraud on government benefits or grants.

Secondary participants, i.e., participants that should be part of the TCRA and provide input but who will not necessarily be part of decision-making processes, include:

- Professional bodies that regulate professions where tax crime risks may arise (e.g., financial services firms, tax advisors, accountants, lawyers, public notaries).
- Representatives of economic or financial sectors that might be considered to have an elevated risk of being used for tax crime purposes (e.g., gambling, real estate, virtual asset service providers, etc.).
- Non-governmental organisations (NGOs), academia, and other members of the public, such as individuals with specific, valuable knowledge on the prevention, detection, and prosecution of tax crimes.
- Even though a whole-of-government representation will be required for a successful TCRA, its preparation will usually be the main responsibility of the tax crime enforcement agency, which is by nature the most appropriate agency for detecting and understanding tax crime risks. Within the tax crime enforcement agency, the most appropriate individuals, as selected by senior management, will conduct the TCRA. It may be helpful to involve others from the tax administration, particularly those involved in compliance risk management, audit and administration reform strategy to help ensure a wider perspective, as well as representatives for other agencies involved in tackling tax crimes and related crimes.

Box 2.2. Participants in the TCRA Framework

Example from Colombia

In Colombia, the Office of the Attorney General is responsible for the investigation and prosecution of crimes pursuant to Article 250 of the 1991 Constitution and Article 66 of the Code of Criminal Procedure.

However, in practice it relies heavily on the filing of criminal complaints and the provision of information and expert evidence by the National Tax and Customs Administration (DIAN). Furthermore, Acts 633 of 2000 and 1762 of 2015, and Executive Order 1742 of 2020 attach POLFA, a body of police criminal investigators focussed specifically on tax and customs violations, to the DIAN. Hence, the Colombian model requires the participation of at least three agencies with a mandate to tackle tax crimes in the preparation of the TCRA.

Preparing a TCRA

Securing high-level support and participation

Ideally the decision to conduct a TCRA should be taken at a high enough level to ensure that all primary and secondary participants take active part in the process. The exact position of the individual(s) that

should take this decision will depend on the institutional framework of each jurisdiction. For example, this might be officials at the level of Commissioner of Taxes, Chief of Police, Attorney-General or Cabinet Ministers. Their decision to commission a TCRA will send the message to all stakeholders of its importance and, ideally, will also involve a call to all relevant agencies to take part in its development. In some jurisdictions, periodic TCRAs with input from all required stakeholders are mandated by law.

Box 2.3. Securing high level support and participation

Example from Chile

The Ministry of Finance in Chile is tasked with directing the financial administration of the State, proposing the economic and financial policy of the Government within its jurisdiction, and co-ordinating and supervising actions executed under such policy. Several public services related to financial administration directly or indirectly fall under the Ministry of Finance, and they are required to co-ordinate all their activities with the Ministry of Finance. Among these services is the Chilean Tax Authority (Internal Revenue Service).

Accordingly, the Internal Revenue Service and the Ministry of Finance must carry out their tasks in a co-ordinated manner, striving for unity of action, avoiding duplication or interference of functions, and ensuring the efficient and proper administration of public resources and the proper fulfilment of public duties.

This co-ordination is overseen by the Ministry of Finance through the Tax Policy Co-ordinator, who systematises both information and the issuance of legislative bills between the two public bodies, particularly when they relate to the oversight of internal taxes.

In accordance with the co-ordination principle, an agreement was signed in 2016 between the Internal Revenue Service, the General Treasury of the Republic, and the National Customs Service, aiming to enhance the efficiency of fulfilling the tax obligations of the country. In accordance with this agreement, a tax subcommittee was formed, as a permanent body with the aim of making the work of the three services more effective in order to reduce tax evasion, fraud, and customs smuggling, and ensuring the proper use of tax, customs, and export promotion franchises, as well as strengthening the co-ordination of the legal powers of the three institutions to generate tax policies aimed at objectives such as reducing tax evasion and avoidance.

Additionally, in order to assure sufficient support to conduct a tax crime risk assessment, the Internal Revenue Service has built a close relationship with the Public Prosecutor's Office, formalised through a Collaboration Agreement signed on June 23, 2023. This agreement specifically establishes effective co-ordination in the criminal prosecution of tax offenses and stipulates that both institutions must exchange statistics, reports of various kinds, and general data analysis related to tax crimes for a more efficient and effective criminal prosecution.

Agreement by all participants

After the decision to launch a TCRA is taken, the process can be streamlined by having key stakeholders agree on the final text/language in writing, for example, through Terms of Reference (ToR) or a Memorandum of Understanding (MoU). The ToR/MoU drafting and negotiation processes would usually be led by the tax crime enforcement agency in consultation with the other primary participants.

The ToR or MoU should critically assess the environment within which the TCRA is being produced. This will include, among other information, relevant legislation, government policy already in place in the field,

management structures and organisations involved, and community expectations in the results. If this is the first time that a TCRA is conducted, it may be of interest to add an agreed provision in the ToR/MoU detailing that the TCRA should be updated after a certain period of time to take account of changes in the environment or an enhanced understanding of certain risks.

The ToR/MoU will also define the scope of the work, which will be tax crime in accordance with the legal definition employed by the jurisdiction. This may include AML/CFT, corruption, bribery or other crimes where there are known strong links to tax crime. The ToR/MoU should also lay down the objectives of the TCRA for example, proactive identification of current and future major threats and assessments of how far they are currently mitigated.

Attention should also be paid to the size and complexity of the economy and of its tax base, the quantity and nature of cross-border financial flows, the size of the shadow economy, the predominance of certain sectors in its national economy and the maturity of its tax crime enforcement framework.

A national TCRA, however, should focus on macro-level risks. For example, looking at the risks posed by particular sectors or actors, rather than naming individual institutions. Similarly, the TCRA might best focus on the overall adequacy of resources to tackle tax crime rather than pointing to individual authorities. It is expected that some renegotiation may take place among primary participants on the final wording of the ToR/MoU, particularly to reflect the risk assessments and strategies produced by those bodies.

In drawing up a TCRA, an important part of the governance arrangements will be to prevent the process from becoming unduly influenced, or subordinate, to a particular policy approach, an institutional agenda, or lobbying from particular stakeholders. Separately, officials involved in preparing the TCRA require professional autonomy as well as the authority to carry out the assessment independently and objectively.

Officials involved in the preparation of the TCRA will also need to recognise openly all the tax crime threats that exist in their jurisdiction, and how these may be different from threats happening in civil/administrative tax matters, the AML/CFT space, or other serious crime. Specific tax crime threats may include underreporting of income, claiming false deductions, setting up legal vehicles to claim undue government benefits, missing trader fraud etc. In other cases, however, tax crime threats may be similar to those related to civil/administrative tax matters, especially when countries' definitions of tax crime focus on monetary thresholds instead of intent.

Further, the TCRA will increase each agency's awareness of where they and other agencies sit as part of a 'whole-of-government' approach to addressing tax crime and possibly, using tax crime legislation as a means to disrupt other criminal activity in the jurisdiction.

Box 2.4. Referral mechanisms between civil/administrative tax authorities and the tax crime enforcement agency

The OECD has been encouraging sharing of information between the civil tax authorities and the tax crime enforcement agency for decades. Already in 1977, the Recommendation of the Council on Tax Avoidance and Tax Evasion recommended that countries strengthen their information exchanges with a view to combatting tax evasion. In 2010, the OECD Council issued a Recommendation that jurisdictions "establish, in accordance with their legal systems, an effective legal and administrative framework and provide guidance to facilitate reporting by tax authorities of suspicions of serious crimes" (OECD, 2024[9]). Finally, the 2022 Council Recommendation on the Ten Global Principles for Fighting Tax Crime, states in Principle 8 that countries should "establish effective legal, administrative, institutional, and operational frameworks for domestic inter-agency co-operation, including reporting and information sharing by tax authorities of suspicions of tax crimes and other financial crimes (OECD, 2022[1]). While OECD Council Recommendations are not binding, they show the political commitment of OECD Member countries, and other adherent jurisdictions, to implement such measures in practice.

As part of the effort to improve referral mechanisms, the OECD has also published two awareness-raising handbooks for tax examiners and tax auditors for detecting possible indicators of bribery and corruption (OECD, 2013[10]), and of money laundering and terrorist financing (OECD, 2013[10]).

Many countries have similar mechanisms in place where a civil auditor can refer an investigation to the tax crime enforcement agency if there are indications of fraud or other crimes. By way of example, in the United States, the Internal Revenue Manual of the IRS describes what the civil examiner should be alert for to detect fraud (Internal Revenue Service, 2023[11]).

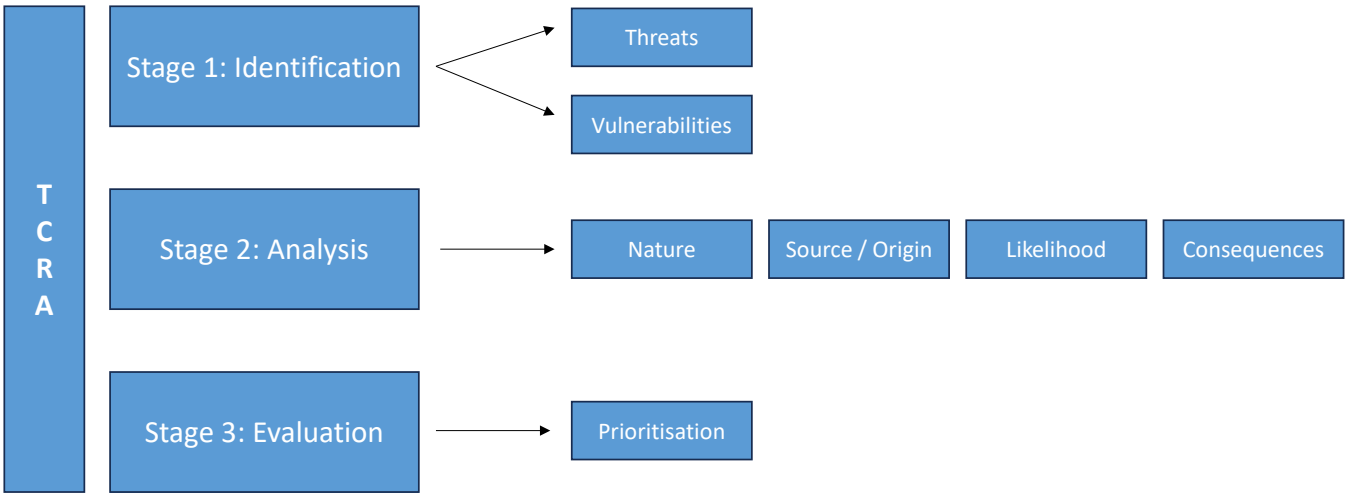
Planning and allocation of tasks

The process can be divided into two stages[2]:

1. **Identification of risks** by developing a list of potential threats and vulnerabilities based on data analysis and/or emerging trends already observed. The identification stage should be as comprehensive as possible. It is however a living stage, in the sense that more threats and vulnerabilities (new or previously undetected) may also be considered in later stages of the process.
2. **Analysis of risks** by analysing the threats and vulnerabilities, considering their nature, sources or origins, likelihood, and impact. The aim of the analysis stage is to gain a complete overview and understanding of the risks, including their consequences, and assign to each risk a relative weight for prioritisation.

The figure below provides a diagram illustrating the planning stages of the TCRA.

Figure 2.1. Overview of the TCRA



Source: This figure has been adapted by the OECD Secretariat from FATF (FATF, 2013[8])

Stage 1: Identification of risks

Analysis requires information. One of the key elements for a successful TCRA is the use of all the relevant sources of information that may contribute to assessing tax crime risks in a jurisdiction. While in some respects the TCRA work may be conducted by a single agency (particularly where the tax crime enforcement agency is housed within the tax administration), it is unlikely that this single agency will possess all the necessary information and data to perform the task. Determining the data sources, types of information and analytical techniques used for conducting the TCRA will be critical for its success.

The availability of sources of information will greatly vary depending on the jurisdiction. Jurisdictions with limited information may have to rely more on expert judgment and on data obtained from international sources, such as that of tax exchanges on request or those made under the OECD Common Reporting Standard (OECD, 2020[12]). Intelligence units, either in house or across government, may also be able to support in collecting data and information regarding risks. Where information gaps exist (for instance, due to lack of reliable data, or where there are legal barriers prohibiting sharing information between certain agencies), they should be acknowledged in the TCRA so as to inform the possible mitigation efforts addressed in the strategy.

Box 2.5. Possible sources of information

The below list provides some databases and sources of information that could be of use for preparing the TCRA. More information on sharing of information between government agencies for the fight against tax crime may be found in the Ten Global Principles (OECD, 2021[13]) the OECD's Effective Inter-Agency Co-operation in Fighting Tax Crime and Other Financial Crimes (OECD, 2017[14]), and the joint OECD-World Bank report on Improving Co-operation between Tax Authorities and Anti-Corruption Authorities in Combating Tax Crime and Corruption (World Bank and OECD, 2018[15]). For the purposes of the TCRA, access to these databases will not necessarily be required, but rather it would be beneficial to obtain general data from the relevant authorities on existing and latest trends, in accordance with confidentiality rules.

Government:

- Company formation/ownership registry
- Land registry
- Registry of citizens
- Tax databases
- Customs and immigration databases
- Police databases
- Judicial databases
- Financial intelligence unit information
- Suspicious transaction report databases
- Social security scheme databases
- Vehicle registries
- Financial regulators
- Bankruptcy court proceedings

Private sector and non-government sources

- Financial institutions
- Virtual Asset Service Providers (VASPs)
- Insurance companies
- Domestic bank account client databases
- Accounting software company client databases
- Information from lawyers and accountants
- AML compliance departments
- Members of the public – both observers through a tip-off function and witnesses
- Publications from global authorities - for indicators of possible risks and how they may be perceived within a jurisdiction

Finally, criminals or ex-criminals can be a valuable source of information, particularly in jurisdictions where there are incentives to share information with the state in exchange for more favourable treatment in the criminal justice system, or where voluntary tax disclosure or amnesty programmes are in place. Offenders usually possess first-hand information on *modus operandi,* such as why certain sectors of the economy or legal vehicles are preferred to commit tax crimes over others. While obtaining information directly from the

offenders can be difficult, indirect methods may exist, including court reports, sentencing and transcript records, etc. The powers of other agencies may also be utilised, such as through undercover operations, surveillance and coercive hearings.

The TCRA will also benefit from the knowledge from all actors involved in the detection and investigation of tax crime. As such, the list of both threats and vulnerabilities will be large and may include situations or measures which are beyond the control of the primary participants, for example arising from offshore risks. These should also be listed, as the strategy may provide the adequate scenario for seeking changes in legislation, organisational culture or securing buy-in from external stakeholders.

Tax crime risks exist when tax crime threats exploit, amongst other things, tax crime enforcement vulnerabilities. The list of risks will therefore go from broad to specific, based on known typologies, data compiled and drawn from existing cases or known schemes.

Irrespective of the sources of information used (qualitative, quantitative, workshops, common knowledge, etc.), officials in charge of identifying risks should always keep an open mind so as to prevent inadvertently overlooking certain threats and vulnerabilities. Once a list of all risks is prepared, the TCRA team can move to the next stage.

Box 2.6. Identifying risks using different data sources

Example from Australia

Operation Protego is an Australian Taxation Office (ATO) led investigation into large-scale GST fraud that was promoted on social media. It involved an individual:

- inventing a fake business
- lodging a fraudulent Australian business number (ABN) application, and
- submitting fictitious business activity statements (BAS) to attempt to gain a false GST refund.

It quickly spread within the Australian community to scale.

The ATO prioritised and took civil compliance action against more than 56,000 perpetrators and actively informed and warned the community of this scheme, clarifying misconceptions and changing the risk proposition. The ATO informed the community that the fraudulent activity has been circulating as online advertising and content, particularly on social media, and the ATO worked with digital platforms to shut down the advertising.

In addition, working with the Serious Financial Crime Taskforce and law enforcement agencies, more than 100 suspected perpetrators have been arrested or had criminal proceedings commenced, including members of outlaw motorcycle gangs, organised criminal organisations, and youth crime.

Since the reporting in the ATO 2022 Annual Report, civil compliance has raised a further $700 million in liabilities, which includes around $300 million in penalties and interest, and stopped $2.7 billion being paid to fraudsters.

Sources:
1. https://www.ato.gov.au/media-centre/correcting-the-record-on-operation-protego
2. https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/refund-fraud/gst-refund-fraud-attempts#Remindersforthecommunity

Stage 2: Analysis of risks

The second stage of the TCRA consists of moving the list of risks from a description to a more comprehensive understanding of the nature, origin, likelihood, and consequences of those risks. The first step in analysing tax crime risks is understanding why tax crime takes place. The main driver of tax crime is fundamentally always financial profit. However, there are additional environmental factors that can increase the likelihood of criminal offending:

- **Lack of enforcement:** If there is a perceived low risk of detection or enforcement of sanctions, then criminals are more likely to engage in tax and other financial crimes;
- **Links with other illegal activities**: Criminals may seek to evade tax to conceal their gains from other illicit activities and to avoid drawing attention to these activities.
- **Quick gains:** The significant amounts that can be made relatively quickly and often across borders through some forms of organised tax fraud, for example carousel fraud, refund fraud or cum-ex schemes.
- **Minimising tax liability**: although tax planning is legal, this can sometimes cross the line into tax evasion.
- **Discontent with the tax system and/or government:** Some people may be motivated by a dissatisfaction or disagreement with the tax system, choosing to evade taxes as a form of protest.

Alternatively, they may also be discontent with government for any range of non-tax related matters, and therefore not want to contribute through the tax system.

- **Perception of general compliance**: Perceived low levels of compliance across the population can lead to higher numbers of individuals viewing non-compliance and even tax crimes as acceptable behaviour.

A situational analysis should include all the relevant factors that will impact on tax crime, both those that decrease its occurrence, and also those that increase it. These factors may in many cases be related to the general situation of a jurisdiction (economic, political, legislative, and environmental factors), and can coincide with vulnerabilities already identified during the previous stage. This can also cover evolutions in tax administration, for example obtaining data directly on taxable transactions, withholding arrangements of improvements in analytics (including through the use of artificial intelligence over time).

Individual factors vary and evolve over time. A good example of this evolution is tax crimes committed through the misuse of cryptocurrencies. The risk of such behaviour taking place will depend on a series of factors as diverse as whether cryptocurrencies are legal in a certain jurisdiction, the rate of acceptance of crypto-currencies in each market, the stability of the local currency, currency controls, and internet access in a certain region as well as policy measures such as the OECD's crypto-asset reporting framework.

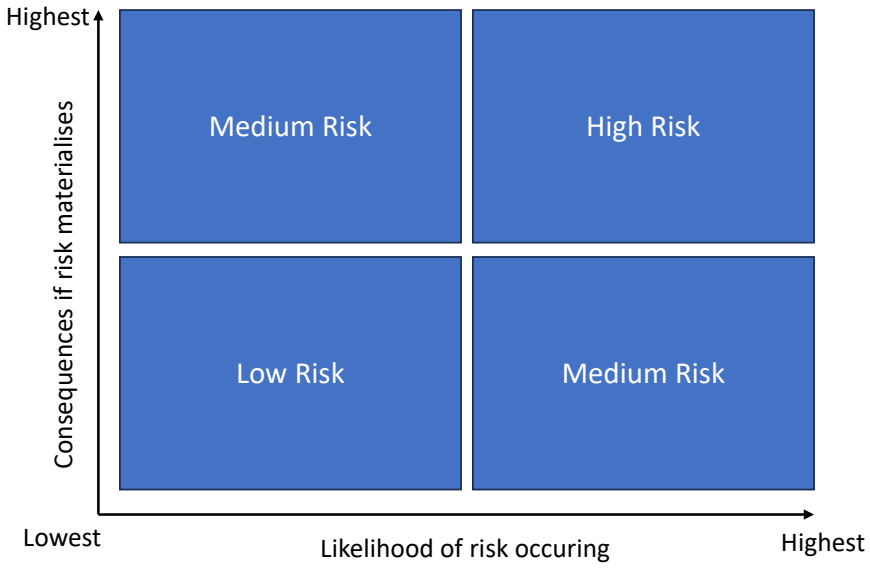
It may become apparent during the analysis stage that some risks were overlooked during the identification process. As mentioned above, the identification stage is a living stage, and new risks may be added (and older risks may be removed) at any time of the process.

One of the possible, non-quantitative inputs for assessing tax crime risks in a jurisdiction is through a series of workshops with all different stakeholders involved in the work against tax crime, both from the public and the private sectors. An example of how to conduct such a workshop follows. This is based on the successful experiences shared by jurisdictions, as well as self-assessment workshops conducted by the OECD Secretariat using the *Tax Crime Investigation Maturity Model* (OECD, 2020[12]):

Evaluation of the risks identified in the TCRA

The likelihood of risks occurring will determine the prioritisation of risks. This part of the analysis can pose some problems as it requires an element of quantitative judgment over data that does not easily lend itself to be used in such a fashion (UNODC, 2010[16]). Given that this is often an inexact science, a valuable tool for prioritising risk is the classic matrix where risk is assessed against likelihood and consequences. In a basic manner, the risk matrix would look like the figure below.

Figure 2.2. Risk matrix



Source: Adapted by the OECD Secretariat from (UNODC, 2010[16])

The risk matrix is a visual tool used to assess and prioritise tax crime risks based on their likelihood and impact. Risks can be plotted on the matrix based on their assessed likelihood and consequences.

The focus should be on the risks located in the high-risk cells of the matrix – these are the risks with both high likelihood of happening and impact. What is deemed to be high risk will vary according to the country, but the table outlines some key considerations for evaluating both the consequences if a risk materialises and the likelihood of the risk occurring.

Table 2.1. Factors to consider when plotting the risk matrix

Consequences if risk materialises	Likelihood of risk occurring
• How many taxpayers use the potential risk? • How much money is at risk? • How many people use or have access to the risk? For example, a social security payment system will have many more users than a narrowly targeted grant scheme. The number of participants then affects the amount of money involved.	• How much control/assurance is being conducted before a loss occurs? • How well is the risk mitigated already. For example, for well-known and long-standing risks, the related vulnerabilities may have already been largely identified and addressed, as opposed to a new and emerging risk. • Is there any time pressure involved? For example, in the case of tax refunds there is limited time to audit a tax return, and this may make it more likely for a loss to go undetected for a period. • Is there adequate resource to review the potential risk? For example, a high flow of claims that need to be approved as soon as possible. • Was the risk something that was designed quickly? For example, if it was a programme designed quickly in response to an urgent external event (e.g. COVID) then there may have been a limited time for staff to review claims, consider vulnerabilities and implement safeguards.

The adoption of three risk levels (low, medium, and high) is subject to each jurisdiction's decision. Some countries have adopted alternative matrixes such as a five-stage level (lowest, low, medium, high, and very high) rather than the three stages provided in this document.

This stage of the TCRA can build on information gathered and identified in the first two stages to provide a risk profile to determine the likelihood and consequences of tax crime occurring and where to prioritise resources upon implementation of the strategy.

It is important that the results of the analysis are written, including a list of all risks and their levels of likelihood. This new document, compiling the identification and analysis stages, will be the first draft of the TCRA, which will then be shared with all primary participants for feedback. The agreed definitive version will be the TCRA.

Box 2.7. Example of a TCRA risk matrix

Example from Sweden

Sweden's risk management model is a tool for the prioritization of risks, and the risk matrix is a fundamental part of this under the risk assessment stage:

- Risk analysis
- Risk assessment
- Actions
- Evaluation

The risk assessment is primarily about evaluating risks and deciding whether a risk needs to be managed to ensure the success of the operation. The risk assessment consists of two parts: consequence and probability. Common scales make it possible to set risks against each other, which is useful when risks are to be compared between different parts of Sweden Tax Authority's (STA) operation.

The risk assessment begins with determining the degree of severity, i.e. the consequence of a certain event or circumstance occurring. The risk assessment of consequences is generally based on four levels of impact on STA´s operation: Insignificant (1), Moderate (2), Significant (3) and Serious (4).

The next step is to assess the probability of the risks occurring based on four levels of probability: Very low frequency/ Unlikely (1), Low frequency (2), High frequency (3) and Very high frequency/ Very likely (4).

Based on the risk assessment each risk can be placed in the following matrix:

Very high frequency / Very likely	4				
High frequency	3				
Low frequency	2				
Very low frequency / Unlikely	1				
Probability of risk occuring		1	2	3	4
Consequences		Insignificant	Moderate	Significant	Serious

Source: Swedish Tax Agency

As a rule, risks placed in the red sectors shall be handled by STA. The risks placed in the yellow and green sectors will be handled if the measures are considered not to be too resource intensive.

Box 2.8. Organising and preparing a TCRA workshop

One of the possible, non-quantitative inputs for assessing tax crime risks in a jurisdiction is through a series of workshops with all different stakeholders involved in the work against tax crime, both from the public and the private sectors. An example of how to conduct such a workshop follows. This is based on the successful experiences shared by jurisdictions as well as self-assessment workshops conducted by the OECD Secretariat using the Tax Crime Investigation Maturity Model (OECD, 2020[12]):

- Organise a three-day workshop with a multi-disciplinary team of participants, which could include the tax crime investigation agency, intelligence agency, financial intelligence unit, officials from various functional areas of tax administration (mainly civil audit or customs if relevant), Prosecutor's Office, other enforcement agencies (such as the anti-corruption authority), policymakers and any other stakeholder that the jurisdiction might consider important.
- Appoint a co-ordinator from the tax crime enforcement agency for liaising with the participants and the facilitators before, during and after the workshop. Before the workshop, the co-ordinator will have collected impressions from all the different stakeholders of the existing tax crime risks in the jurisdiction.
- Appoint two facilitators, who may not necessarily be officials of any of the agencies participating, who will facilitate the discussions during the workshop.

Conducting a TCRA workshop

- Sufficient time should be allowed for discussion during the three-day workshop, as to deliberate the best evaluations for each threat and vulnerability.
- The facilitators will set the ground for the discussions by introducing the main components of risk (threat, vulnerabilities, and consequences) as well as the different between threats (external) and vulnerabilities (internal).
- Divide the participants into several groups, ideally diversifying agencies and roles in the group, and assign each group to a small series of risks as identified by participants before the workshop.
- Each group is to discuss the different risks as identified before the workshop. They will debate whether the previously identified risk stand and identify new risks.
- To be effective, the exercise should be done in a way which makes the process as objective as possible and inspire critical thinking. Care should be taken, though, to ensure that the conversations can be frank and open, and people should be encouraged to express their views.
- At the end of the workshop, a record sheet is prepared by each group, indicating the risks as identified. Each group makes a presentation at the end of the workshop with a detailed analysis of the risks they identified, along with the risk level measured. Conclusions drawn by a group should be challenged by another group during presentations.
- It is a good practice for the facilitators to challenge the views of the including asking for supporting evidence where appropriate during the presentations made by each group.
- Outcomes of the TCRA workshop.
- A final record sheet is prepared after combining all the assessments made by each group and a set of recommendations for improving effectiveness in the jurisdiction.
- The co-ordinator submits a report to the head of the tax crime enforcement agency on the workshop including the risks assessed, and recommendations made by the participants.

- The reports of the different workshops will be used as input for the preparation of the tax crime strategy.

Notes

[1] Of particular interest are the *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment* and the UNODC's *Guidance on the preparation of serious and organised crime threat assessments ("The SOCTA Handbook").* Noting that in most jurisdictions tax crime is a predicate offence for money laundering, this document has tried to follow the FATF methodology and guidance, while noting that in some instances a TCRA will present differences from an AML/CFT risk assessment.

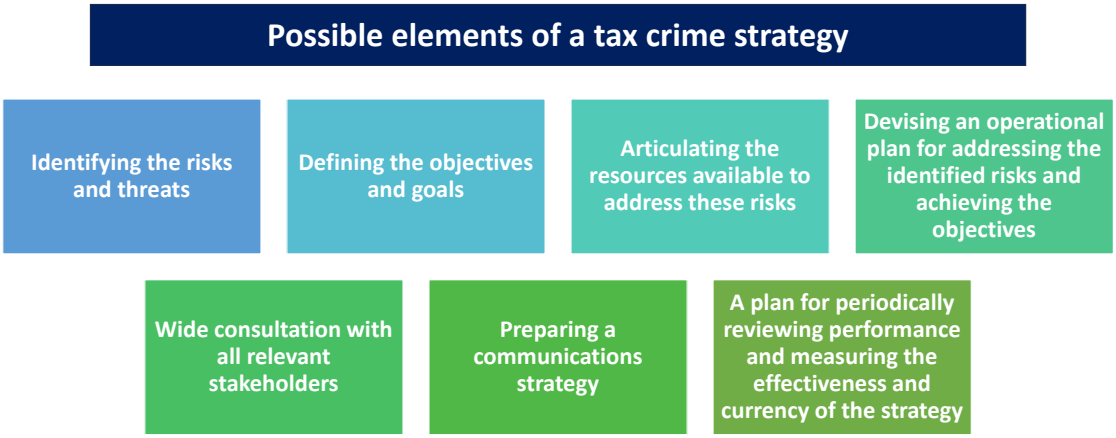
[2] A more detailed guidance on how to produce a threat assessment against serious organised crime, which is in a large manner applicable to TCRAs, is available from the UNODC's *SOCTA Handbook* (UNODC, 2010[16]).

3 Developing the Strategy

The results of the risk assessment, including the identification and analysis of risks, should feed into the tax crime strategy which will provide practical solutions to address the risks. As tax crime risks are now properly understood, jurisdictions can apply proper measures to counter criminal activity in a way that is proportionate with the detected risks.

This chapter sets out some of the key elements that officials may want to consider when developing their tax crime strategy. There are, of course, different ways to design an overall strategy, depending on a jurisdiction's individual circumstances.

Figure 3.1. Possible elements of a tax crime strategy



Source: OECD 2024

Defining the objectives and goals of the tax crime strategy

Having identified and prioritised the risks, the objectives and goals of the strategy should be defined.

A tax crime strategy's high-level objectives will usually cover the core elements of prevention, detection, disruption, enforcement, as well as the recovery of proceeds linked to the tax crime. However, what that means in practice will vary according to the country. Objectives may be set according to the key risks identified in the TCRA, explicitly bringing out the linkages between objectives set by various enforcement agencies dealing with financial crimes as well as the tax administration's overall strategy (OECD, 2020[12]).

When drafting the objectives of the strategy, it is also helpful to include a set of clear and measurable goals that can help others such as officers and investigators understand what they are trying to achieve through the strategy. These might naturally be set out under each of the objectives. Setting out objectives of where the tax crime agency and jurisdiction wants to be in the future – 'the vision' – and outlining how it wants to achieve its goals – 'the plan' – will help focus the attention of relevant stakeholders on key priorities and responsibilities.

Where the strategic plan is published, the administration can be held accountable for the achievement of the goals. Whilst being ambitious, the goals also need to be realistic. Attention should also be paid to what is being measured. Sometimes if the goals are too narrowly metric focused, then they can miss the overall outcome the jurisdiction is trying to achieve.

Jurisdictions may wish to consider using SMART goals in this respect, i.e. goals which are specific, measurable, achievable, relevant, and time-bound.

Officials drafting the strategy may also wish to consider having objectives that cover different time periods (short term vs. long term). Short term objectives would look at, for example, the coming year and should give a first indication of whether the strategy is successful or not relatively soon after implementation. Medium and long-termer objectives as to how to impact tax crime may be more aspirational in nature and, in an ongoing changing environment, may require adjustment over time, including as new technology tools become available.

Developing an operational plan

Based on the risks identified in the TCRA, the strategy will consider the best way to address those risks through an operational plan. Different risks will require different approaches. Depending on the origin of the threat, jurisdictions may wish to consider approaches in the following three categories.

Figure 3.2. Core elements for addressing identified risks

Source: OECD

- **Prevention** relates to mechanisms that prevent a certain activity from occurring, for example, through greater controls over activities, engagement with at-risk sectors or through the design of systems. For example, if a country is facing risks related to the misuse of cash, it may decide to impose a threshold on cash transactions, and/or to set out tax benefits for using other payment methods such as debit or credit cards. Voluntary disclosure programmes could also be deployed (where taxpayers come forward and self-report to avoid penalties) and would have the benefit of reducing the demand on resourcing. Looking at system design could also be beneficial where there are risks of weaknesses being exploited. In addition, the tax crime enforcement agency can develop a programme of engagement, including through other agencies, regulatory authorities and professional bodies, with at risk sectors or those conducting activities identified as a potential risk.

- **Enforcement** includes detection, investigation and eventually the criminal prosecution and sanctioning of certain activities. This usually involves high-level risks as per the risk matrix, where not only is there an elevated likelihood of them taking place, but their consequences are such as to justify stronger actions. These risks therefore require immediate action and the full use of available legal powers. Rather than focusing on single entities or individuals, the strategy should focus on certain sectors of the economy which are deemed high-risk. This may include, for instance, sectors of the economy which are considered of national interest, or that are known by law enforcement to be used by criminals not only for committing tax crime offences, but also to launder proceeds of crime, or to finance other illegal activities. Enforcement has obvious benefits in terms of deterring others who may be considering engaging in similar illegal activities and maintaining the integrity of the tax system by holding people accountable for their actions. Approaches should also consider the effective allocation of human and technological resources or a combination of both to addressing the observed risk.

- **Contingency planning** refers to risks which have been detected during the course of the TCRA, but were determined too low to enable or require immediate or targeted action. This may occur due to a series of factors such as their consequences being assessed as low, and/or the risks relating to a specific, short-term policy decision. As resources are scarce, it may be decided not to allocate them to countering these risks. However, the risks are still present in the jurisdiction, and they should be subject to increased monitoring, with the view of raising their risk level if they do not end over a brief period of time. The benefit of contingency planning is that the risk is known from the outset and the TCRA provides a platform for agencies to consider what intervention they may take in the future if the risk moves higher in the matrix, or there is increased capacity to address risks. Identified risks may require a combination of the methods above to address them. For example, prevention measures might work against more opportunistic actors, whilst prosecution could be required for the more persistent actors who continue the behaviour.

Jurisdictions may also want to consider having an early warning system that guides detection and prevention of crimes as part of the plan to address and mitigate risks. This could be supported by predictive analytics and artificial intelligence to forecast different scenarios that should be taken into account (OECD, 2020[12]).

Box 3.1. Devising an Operational Plan

Tax crime risks as part of the National Fraud Strategy

Example from Spain

Each year, Spain's tax administration agency updates and publishes a 'Plan of Tax and Customs Control'. The plan is centred around five main actions – tax and customs fraud control, tax and customs investigations, promoting voluntary compliance, promoting the use of online services, and enhancing information exchange practices with the tax agencies of the 17 Spanish autonomous communities. This strategy is informed by inputs from other financial crime authorities, including the Anti-Corruption Prosecutor.

For 2020-23, the main targets set out in the strategy include tax compliance in large companies; analysis, intelligence-gathering and investigations in cases of fraud; the fight against smuggling, particularly of tobacco; and the analysis of money laundering associated with customs offences.

Source: https://www.oecd.org/tax/crime/fighting-tax-crime-the-ten-global-principles-second-edition-country-chapters.pdf

Tax Crime Risks as part of HMRC's Strategy for Offshore Tax Compliance – No Safe Havens

Example from the United Kingdom

HMRC's strategy for offshore tax compliance – No Safe Havens 2019 - brings together in one place HMRC's approach towards offshore tax compliance. HMRC has a strong track record in tackling offshore non-compliance, whether stopping this through leading international activity, providing easy ways for people to disclose correct their tax affairs, or by acting against those who are intent on breaking the law.

No Safe Havens 2019 covers a range of behaviours, from simple mistakes to avoidance and evasion. The strategy sets out how HMRC will ensure offshore tax compliance and tailor our approach, helping customers get it right first time where possible. Where HMRC intervene, they will use an approach that is appropriate and proportionate to the tax at risk and the customer's behaviour. HMRC also leads international work to improve tax transparency initiatives which provide data crucial to tackling offshore tax evasion.

Since the No Safe Havens Strategy 2019 was introduced, HMRC have secured around £621 million from offshore initiatives, underlining its commitment to tackle all forms of non-compliance and ensure the right amount of tax is paid, to fund the UK's vital public services.

This has helped ensure that the UK tax gap is at a near record low and transformed HMRC's approach to offshore tax. Measures introduced to tackle offshore evasion include new offences and increased sanctions for those who seek to evade tax, as well as those who help them. Time limits to allow HMRC to investigate and settle liabilities relating to offshore tax offences have been doubled compared to time limits for investigating domestic tax offences. Similarly, financial penalties for offshore tax offences have been doubled compared to those for onshore tax offences.

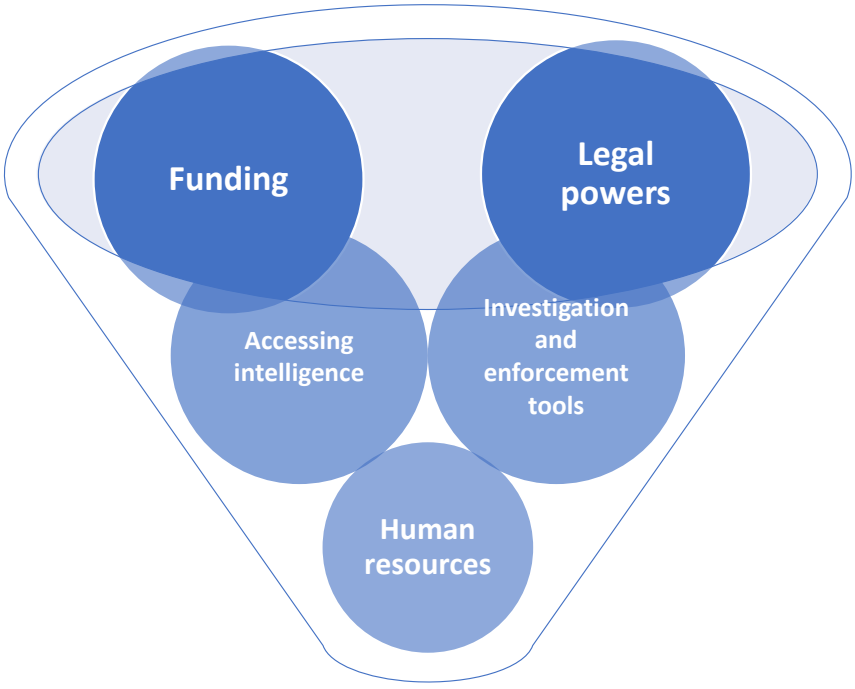
Sources:
1.https://assets.publishing.service.gov.uk/media/5cdd3d8940f0b650cf39296b/No_safe_havens_report_2019.pdf
2. https://www.gov.uk/government/statistics/measuring-tax-gaps

Available Resources

To develop an operational plan, it is important to fully understand the context within which the tax crime enforcement agency and relevant stakeholders operate.

The first thing to establish is the resources and tools available to address the identified risks as well as to consider possible vulnerabilities in their available resources, and identify any gaps and weaknesses. The main elements are set out by the diagram and outlined in more detail below:

Figure 3.3. Available Resources



Source: OECD

Legal powers

The legal powers available to a jurisdiction underpin its ability to effectively fight tax crime and related crimes. One of the overarching purposes of a tax crime strategy is to ensure that the laws related to tax crimes are effective in practice, and the jurisdiction has a set of legal powers available that are adequate to enforce these laws. They include the necessary authority to collect information, investigate, prosecute, in addition to collaborating with stakeholders, both domestically and internationally.

Criminal law enforcement will be a particularly important part of this. Depending on the jurisdiction, the criminal law enforcement branch responsible for tax crime may sit within the tax crime agency or outside

it. If it is outside it, investigative capabilities may not be available to the tax crime agency. Jurisdictions should give careful consideration to how they co-ordinate to ensure that any available legal powers are maximised in this case. Ideally, legal powers will be fairly expansive to enable information sharing between agencies, without undue restrictions and cumbersome authorisation processes.

Access to wide-ranging intelligence sources

Information sources are also covered in chapter two on TCRAs, but it is significant to note here that ideally there will be access to a wide range of intelligence sources (both domestic and international), intelligence from other enforcement agencies, financial intelligence from the FIU, financial regulators, third party information on transactions and open-source intelligence (including social media). Some of these may require resources to access, potentially including the development of IT and analytic tools. Over time, artificial intelligence may also increasingly be used to determine actionable intelligence, by seamlessly linking intelligence sources (OECD, 2020[12]).

More information on inter-agency co-operation can be found in the OECD's Effective Inter-Agency Co-operation in Fighting Tax Crime and Other Financial Crimes (OECD, 2017[14]), and the joint OECD-World Bank report on Improving Co-operation between Tax Authorities and Anti-Corruption Authorities in Combating Tax Crime and Corruption (World Bank and OECD, 2018[15]). Jurisdictions may also wish to undertake a self-assessment on using the inter-agency trust maturity model contained in the OECD's report, Enhancing Inter-Agency Trust Between Tax and Other Financial Crime Authorities (OECD, 2023[17]).

Investigation and enforcement tools

Successful investigations are paramount to uncovering tax crimes and the eventual prosecution or deterrence of such crimes. Jurisdictions may wish to review their powers by undertaking a self-assessment using the OECD's Tax Crime Investigation Maturity Model (OECD, 2020[12]).

Box 3.2. OECD Tax Crime Investigation Maturity Model

The Maturity Model is a tool developed for jurisdictions to self-assess their capabilities to investigate tax crimes and facilitate their tax compliance efforts through capacity building. Based on the OECD's 2017 publication, Fighting Tax Crime: The Ten Global Principles, the model charts out an evolutionary path across four levels of maturity: Emerging, Progressing, Established and Aspirational, to show how enforcement capabilities are enhanced through continuous process improvement and holistic implementation of each of those principles. The processes used for implementing the Ten Global Principles are used as the objective criteria for mapping the maturity level in a jurisdiction. These are processes that have been identified across multiple jurisdictions, which have helped to achieve defined outcomes and the overall objective of the tax crime investigative agencies. At higher levels of maturity, the tax crime investigation regime is effective, supports the integrity of the tax system and Sustainable Development Goals (SDGs) of domestic resource mobilisation and countering illicit financial flows (IFF).

Self-assessment through the Maturity Model is a purely voluntary exercise. The Model does not set any new global minimum standards which the jurisdictions are expected to follow. The Maturity Model analyses how a jurisdiction can mature in its ability to fight tax crimes, rather than simply describing

what occurs within the tax crime investigation regime. This capacity-building focus is integral to the Maturity Model, in recognition of the Addis Tax Initiative and G7 Bari Declaration, but it is of relevance for jurisdictions at all stages of development. The Aspirational level of maturity focuses on futuristic attributes, making it relevant for the advanced jurisdictions.

Source: OECD Tax Crime Investigation Maturity Model (OECD, 2020[12])

Figure 3.4. Investigation and enforcement tools

Source: Adapted by the OECD Secretariat from (OECD, 2020[12])

These powers should have extensive procedural safeguards and oversight in place to ensure the rights of individuals and suspects are maintained and do not jeopardise an investigation.

Resources

Detecting, investigating, and prosecuting tax crime offences of course results in a cost to the state budget. Jurisdictions should identify and prioritise areas that require funding, such as:

- **Skills**: Recruiting and retaining skilled investigators, auditors and legal experts.
- **Technology**: Investing in cutting edge technology and analytical tools.
- **Infrastructure**: Ensuring that the necessary infrastructure is in place to support intelligence gathering, detection, and investigative efforts, such as secure databases and communication systems.
- **Training**: Allocating funds for training programmes to enhance the skills of tax authorities, financial intelligence units and law enforcement personnel involved in tacking tax crimes. Training may also be relevant for private sector participants involved in the front-line detection of tax crimes.
- **Law enforcement**: Costs incurred through the investigation of tax crimes.
- **Criminal justice**: Costs related to charging, prosecuting offenders, and sanctioning offenders, such as the resources required by the prosecution service, courts, legal defence aid, and the probation and prison services.
- **International collaboration**: Support participation in joint initiatives, taskforces, information-sharing platforms and training programmes organised by global entities.
- **Communication strategies**: Funds to educate the public about the consequences of tax evasion and the importance of complying with tax regulations.

It is unlikely that tax crime enforcement agencies will be able to fund all these areas to the extent that they would like to, and so they will have to prioritise which are most important according to the context of the jurisdiction, appropriate and proportionate to the identified risks.

It will also be important to get budget holders to support the strategy, both within the tax crime agency and wider government, as ultimately, they control how much money the agency will receive and how much can be budgeted for implementing the strategy. Here it will be important to demonstrate that the strategy offers value for money.

Human Resources

Trained personnel are essential for the effective implementation of tax crime strategies. They will come with a range of backgrounds and professions, such as law enforcement, investigation, financial analysis, legal, data analysis, technology and civil servants. Expertise, experience, and a deep understanding of complex financial systems, legal frameworks and evolving methods used by individuals and businesses to evade taxes is also crucial to effectively disrupt tax crimes.

Jurisdictions may want to consider introducing flexibility to the recruitment process by allowing for the recruitment of skilled personnel from other government and enforcement agencies on a secondment basis. Conducting joint investigations with other domestic agencies or international partners, where appropriate, may also enable the pooling of resources and knowledge sharing between experts.

Structured mandatory training for officials may also be helpful, with a specific budget allocation for training. In addition, continuous professional development could be integrated into the structured training, alongside the facilitation of cross agency and international exercises/ exchanges. For example, the OECD runs an Academy for Tax and Financial Crime Investigation, aimed at equipping financial investigators with the tools and techniques needed to combat tax crimes and related crimes effectively.[1]

Domestic Stakeholder Collaboration: A whole of government approach

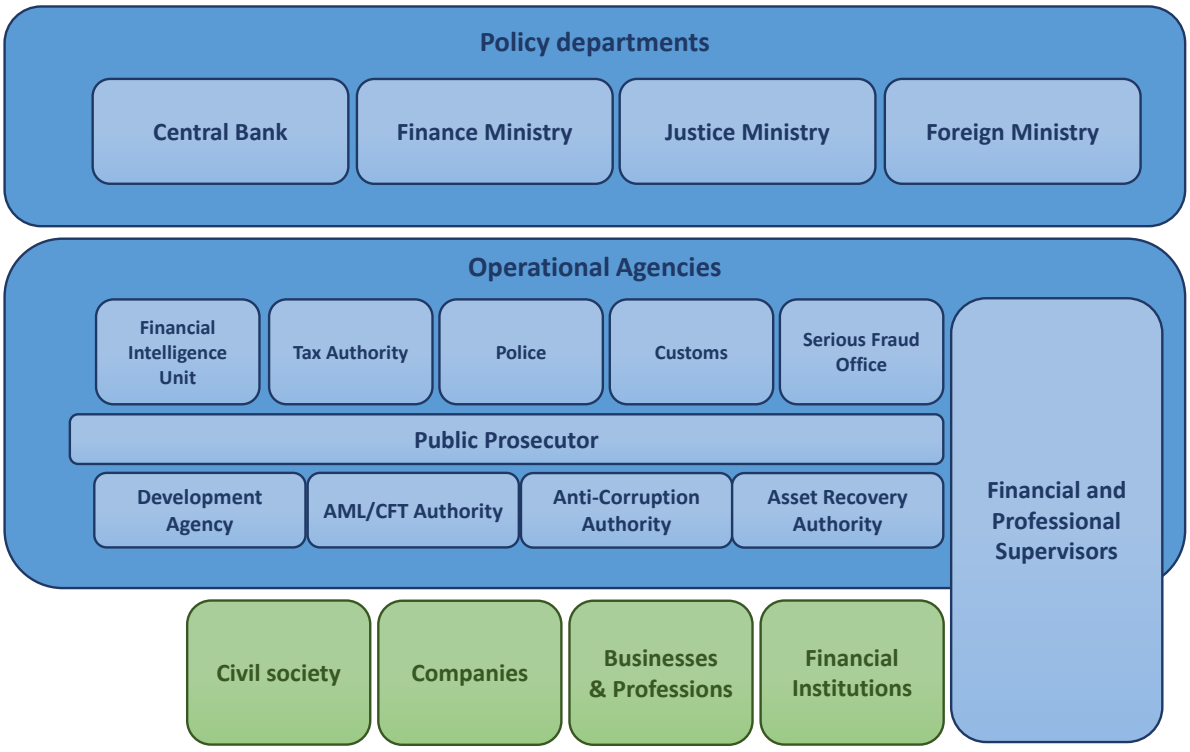
It is important that the strategy is based on wide consultation with all relevant stakeholders, such as revenue agencies, policy makers, investigators, enforcement and prosecution officials and other agencies

such as Anti-Money Laundering Authorities, in accordance with each jurisdiction's legal system, policy and legislative environment and general structure of law enforcement (OECD, 2021[13]).

Co-ordination and co-operation among participants will become crucial as disruption efforts will involve different agencies. Input from the private sector, particularly the financial sector, will also be relevant as they should be able to update their detection and reporting mechanisms considering the risks detected and the strategy's action plan.

The list of key stakeholders will vary according to the jurisdiction, as each has a unique organisational structure and set of agencies.

Figure 3.5. Key actors to involve in a whole of government tax crime strategy



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.
Source: (OECD, 2023[17])

Jurisdictions should implement whole-of-government approaches where possible, in line with the Ten Global Principles (OECD, 2021[13]). This approach emphasises collaboration and co-operation across the various operational agencies, policy departments and ministries. A core component of an effective whole of government approach is inter-agency trust. More can be found on this in the paper *Enhancing Inter-Agency Trust Between Tax and Other Financial Crime Authorities* (OECD, 2023[17]).

Although there is no one size fits all approach for engaging with stakeholders, the first step should always be to identify who the key stakeholders are.

Figure 3.6. Stakeholder engagement: A suggested guide

Source: OECD

It is also important that the strategy for addressing tax crimes includes a mechanism for tax crime investigators and civil/administrative tax investigators/auditors to share expertise, processes and intelligence. This is because the officials responsible for non-criminal matters and for criminal matters will often be looking at similar behaviours and actions. The nature and scope of the crimes will massively vary, and it is important that the right agency gets passed the relevant risks as it will have the powers to investigate them.

Setting up operational taskforces with all the relevant agencies may be a useful way to tackle specific or thematic problems, and encourage collaboration across agencies. These could be targeting a specific issue or a standing taskforce to combat tax crime. Even in operational taskforces, it may be helpful to include non-investigative actors such as policymakers and prosecutors.

Strategic co-ordination between the criminal and non-criminal tax officials can help to ensure a coherent use of resources, efficient prioritisation of cases and avoid duplication of efforts by both the tax administration and criminal law enforcement officials (OECD, 2017[14]). Most jurisdictions have a legal requirement for civil tax officials to refer suspicions of tax crimes to the relevant law enforcement authority. There are a number of key factors which can ensure the effectiveness of this process, which jurisdictions might want to include in their tax crime strategy:

- Training for civil tax officials to be able to identify indicators of a crime.
- Having a clearly identified and central point of contact for sending referrals.
- Using a standard form that ensure all relevant data is captured for use by the criminal investigation authority.

- Meetings for feedback between the civil and criminal investigators to improve the quality of referrals.

Box 3.3. Stakeholder collaboration

An example from Indonesia

In Indonesia, one of the key stakeholder collaboration relationships is between the Directorate General of Taxes (DGT) and the Supreme Court. The Supreme Court is considered an important stakeholder because of its role in controlling adjudication of tax crimes. The problem of adjudication often arises when there are different views in the implementation of the law due to different interpretations and understanding in handling tax crime cases. As a result, the quality of the judicial process may become ineffective, unjust, and inefficient.

To mitigate those issues, DGT and the Supreme Court hold short courses for judges on tax crimes, to gain a better understanding of tax law enforcement and the relevant procedures. Participants and speakers from other law enforcement agencies such as the Police Official and General Attorney are also invited, to give a comprehensive picture of how tax investigations are conducted. This is with the intention of broadening and aligning knowledge and understanding of tax crime law enforcement among these agencies.

Additionally, the DGT and Supreme Court have both drafted guidelines for handling tax crime offences in the form of the Supreme Court Directive. The first guidelines were issued in 2021, with a revision expected to be completed in late 2024. The revision will cover all guidance needed to minimise disparities not only in the judicial convictions imposed by judges, but also in ensuring the inclusion of the perspectives of investigators and public prosecutors prior to adjudication.

Box 3.4. Referral mechanisms between civil/administrative tax authorities and the tax crime enforcement agency

The OECD has been encouraging sharing of information between the civil tax authorities and the tax crime enforcement agency for decades. Already in 1977, the Recommendation of the Council on Tax Avoidance and Tax Evasion recommended that countries strengthen their information exchanges with a view to combatting tax evasion. In 2010, the OECD Council issued a Recommendation that jurisdictions "establish, in accordance with their legal systems, an effective legal and administrative framework and provide guidance to facilitate reporting by tax authorities of suspicions of serious crimes." Finally, the 2022 Council Recommendation on the Ten Global Principles for Fighting Tax Crime, states in Principle 8 that countries should "establish effective legal, administrative, institutional, and operational frameworks for domestic inter-agency co-operation, including reporting and information sharing by tax authorities of suspicions of tax crimes and other financial crimes. While OECD Council Recommendations are not binding, they show the political commitment of OECD Member countries, and other adherent jurisdictions, to implement such measures in practice.

As part of the effort to improve referral mechanisms, the OECD has also published two awareness-raising handbooks for tax examiners and tax auditors for detecting possible indicators of bribery and corruption (OECD, 2013[10]), and of money laundering and terrorist financing (OECD, 2013[10]).

Many countries have similar mechanisms in place where a civil auditor can refer an investigation to the tax crime enforcement agency if there are indications of fraud or other crimes. By way of example, in the United States, the Internal Revenue Manual of the IRS describes what the civil examiner should be alert for to detect fraud (Internal Revenue Service, 2023[11]).

International Co-operation: Identification of key cross-border stakeholders

A successful strategy will not only require co-ordination and co-operation amongst multiple stakeholders, but also enhanced mechanisms for international co-operation. For international co-operation, jurisdictions may wish to give priority to jurisdictions with which they already have strong financial flows. Tax crimes are increasingly international in their components, and limitations in co-operation between countries could ultimately result in vulnerabilities being exploited. Bilateral co-operation instruments such as MoUs may also be helpful, particularly with jurisdictions identified as having a high risk of cross-border tax crime.

Box 3.5. Successful cross-border collaboration by the European Public Prosecutor's Office

In response to the fragmented approach of EU Member States vis-à-vis the most serious forms of cross-border VAT fraud, the European Public Prosecutor's Office (EPPO) was established for investigating, prosecuting and bringing to judgement the perpetrators of, and accomplices to, such offences in the jurisdiction of twenty-two Member States. By virtue of its supranational nature, this single office ensures an integrated criminal response against PIF-focused criminal groups and stores the criminal cases files within a single digital repository.

In the context of extensive and intricate investigation information, EPPO wanted to maintain oversight over VAT fraud by collecting, structuring, integrating, and clustering all of the available data. As a result, real-time images of the most serious VAT fraud supply chains were recreated, enabling EPPO to identify key trends and most importantly, identify High-Value Targets (HVTs). Focusing on HVTs impacts criminal organisations and facilitates the recovery of stolen assets.

Focusing on HVTs has led to the setting up of transnational and multi-disciplinary investigation teams composed of prosecutors, investigators and analysts from multiple EPPO Member States, following an integrated investigative strategy. Notable successes include Operational Admiral, where EPPO uncovered organised crime groups responsible for VAT fraud estimated at €2.2 billion.

Preparing a communications strategy

Communication is also a key element for the successful implementation of a tax crime strategy. Developing a communication plan to ensure that the content of the strategy is disseminated effectively within government to internal stakeholders and to external stakeholders will be helpful. An open and transparent communication strategy can help build trust among all parties involved.

Internal communication

Getting buy-in from all levels with the internal stakeholders involved in formulating the strategy is important, as this will allow each agency to adjust and adapt its operational framework to the risks detected as well as to take account of the objectives and goals detailed in the strategy. Additionally, some staff members may have to change the way they do their day-to-day work, adapt behaviour, or learn to handle new technologies and tools.

An effective way of getting buy-in can be through senior management explaining the objectives and why they are so important, promoting the strategy among staff members and detailing how staff can contribute to the process. With more operational staff, it may also be helpful to tailor communication of the strategy to the intended deliverables, whilst still trying to convey how their team's work feeds into the broader strategy. These tailored communication approaches might be more effective as separate documents to the strategy which can be adapted to the audience and give more detail on their role in implementing the strategy. Staff members will likely be more proactive and engaged if they understand the purpose behind suggested changes and see how their work contributes towards the strategy.

It is also important to have effective two-way communication. In this regard, management may wish to facilitate discussions with staff members in building the strategy to help ensure that staff questions are answered, and that any potential implementation issues are identified at an early stage so that they can be addressed quickly and efficiently. In addition, this approach could also allow information to feed up from the operatives through management to the strategy makers so that developments on the ground are noted and the evolution of risks is considered.

External communication

At the same time, there should be a plan for communicating the strategy with the public. This will be important to shape public perceptions and behaviour, as it can be a reminder of the serious criminal sanctions that can be imposed, and function as a deterrent when high profile cases are prosecuted. It can also help to educate the public and build public confidence in the fair enforcement of tax laws.

The best mechanisms for communicating with the public will vary between countries, as well as over time. A multi-faceted approach is likely to be best, and the following could be considered:

Figure 3.7. Communicating the strategy

Targeted

- The administration should be clear who is the target of the communication as this will affect the choice of channels, the tone of messaging and the content of messaging. Without clarity on who the message is for, taxpayers could resent having spent time understanding that it does not apply to them.

Action oriented

- The communication should have a clear point to it, setting out what the taxpayer is supposed to do in the case of reminders of upcoming deadlines or legal changes or what they should take out of the message (for example that compliance and supporting fairness is taken seriously).

Respectful

- Communication should be respectful of the taxpayer, including recognising that what they are being asked to do or to focus on is only one part of the large set of things involved in running a business.
- Ideally, the tone of communication should create an impression that the administration is trying to support the taxpayer to get tax right and reduce burdens.

Goal driven

- The administration should have clear aims for the chosen communication and, ideally, the ability to measure impacts. Goals may be related to upcoming events, such as filing and payment deadlines, or longer-term, such as messaging to reinforce the importance of paying taxes.

Engaging

- In a crowed communication environment, it is important that the communication is noticed and the right channels are used to attract the intended audience.

Timely

- To be impactful, communication has to be immediately relevant to the SME taxpayer. For example, communication well in advance of deadlines may not get noticed or acted upon. In other contexts, such as registration drives, timeliness may be related to the optimum use of a suite of communication channels in order to reinforce messaging.

Easy to understand

- Plain language should be used, avoiding jargon or uncommon undefined terms. Short sentences and concise sentences can also help aid understanding. Consideration should also be given to the position of non-native speakers and the possibility of translating the communication into appropriate languages.

Dependable

- Taxpayers must be able to trust the information circulated by tax administration. It is important to avoid ambiguity and to direct the taxpayer to appropriate sources for more in-depth information. The reputation of the tax administration could be at risk if wrong or misleading information is shared. An increasingly important consideration here is how to ensure that the messaging can be properly identified as coming from the administration and not from fraudsters.

Source: (OECD, 2023[18])

The best mechanisms for communicating with the public will vary between countries as well as over time. This may be an area where sharing good practice between jurisdictions on the pros and cons of different approaches can be valuable.

Box 3.6. Communicating the strategy

'Education to Economic Legality' – A Guardia di Finanza and Ministry of Education joint project

Example from Italy

The "Education to Economic Legality" project has established a communication strategy aimed at raising young students' awareness of the values of economic and financial legality, and showcasing the activities of the Guardia di Finanza to protect institutions and citizens.

This project is based on a Memorandum of Understanding signed with the Ministry of Education, University and Research on 28 October 2011 and renewed on 24 September 2019, with the purpose of promoting the cited values among students and spreading core Italian constitutional principles.

The initiative includes training meetings held by Corps Officers and Inspectors at primary, secondary and high schools across Italy. The topics covered, which are explained in easy-to-understand language and tailored according to the age of the group, highlight the tasks of the Guardia di Finanza as an economic-financial police force focused not only on the fight against tax evasion and fraud, but also on the protection of public spending. Seven editions of the programme have taken place, involving approximately one million students from over ten thousand schools.

The project, suspended since 2020 because of the Covid pandemic, will soon be reintroduced within the framework of a new Memorandum of Understanding with the Ministry of Education and Merit, whose contents are currently being examined and evaluated.

Finally, as part of the mentioned Protocol, a contest called "Together for Legality" has been organised. The participation is opened to all primary, secondary and high school students in the country. The scope of this further initiative is to encourage students to discuss, reflect and develop the topic of the economic and financial responsibility. Participating students are asked to develop (individually or in groups of up to 5 students), by choice, an essay in different expressive forms (e.g. drawing, comics, short film, music clip and photo-montage).

Communicating enforcement actions

Example from Canada

The Canada Revenue Agency (CRA) advises the media and the public of cases involving individuals and/or businesses convicted in the courts of offences under the Income Tax Act, Excise Tax Act, and/or Criminal Code through enforcement notifications. The CRA may also, on occasion, release prejudgment information at different stages of a criminal investigation or prosecution, including, but not limited to, the execution of a search warrant, seizure of assets, and/or the laying of criminal charges.

Enforcement notifications are published on the compliance actions table on the Canada.ca website, promoted through social media, and sent out through the national or regional newswire services, and the electronic mailing list. The CRA will consistently, as much as possible and unless there are court instructions to the contrary, issue an enforcement notification that names the individuals and/or businesses when publicising enforcement actions.

The CRA publishes information about possible tax non-compliance schemes and enforcement actions to encourage voluntary compliance, to demonstrate its commitment to administering and enforcing Canada's tax laws, and to taking action against those who do not comply.

Sources:

1. https://www.canada.ca/en/revenue-agency/news/newsroom/criminal-investigations-actions-charges-convictions.html?utm_campaign=not-applicable&utm_medium=vanity-url&utm_source=canada-ca_cra-convictions

2. https://www.canada.ca/en/revenue-agency/news/e-services/canada-revenue-electronic-mailing-lists/electronic-mailing-list-enforcement-notifications.html

Communicating the strategy: The 'Dirty Dozen'

Example from the United States

Each year, the IRS issues a list called the "Dirty Dozen" of tax scams during each filing season. The list is intended to provide – among others - taxpayers, financial institutions, and tax return preparers an alert of active scams being perpetrated by professional fraudsters.

The list provides a wide range of known scams actively known to the IRS that both taxpayers and tax return preparers should be aware of during filing season. The list includes such items, among others, as false claim scams marketed as a means to eliminate taxable income and also scams perpetrated to steal their identity. The timeliness is beneficial for taxpayers during tax filing season as they receive increased inquiries, offers, and solicitations for assistance. It also serves to remind taxpayers to be diligent about protecting their personal identifiable information not only during tax season, but also yearlong as bad actors continually attempt to obtain their information for nefarious purposes.

The scams identified by the IRS are specific to the US Tax Code and may not be applicable to other countries but can provide examples of potential vulnerabilities in other tax systems. Several scams involving fictitious credits and deductions are relatively simple scams and available for use by a large number of taxpayers. Other schemes are more sophisticated and promoted to wealthy taxpayers and businesses and can be applicable to other jurisdictions. Examples of these scams include the use of complex offshore structures – trusts and insurance products – and accounts to hide income from taxing authorities.

Source:https://www.irs.gov/newsroom/irs-wraps-up-2023-dirty-dozen-list-reminds-taxpayers-and-tax-pros-to-be-wary-of-scams-and-schemes-even-after-tax-season

Notes

[1] More information on the OECD Academy for Tax and Financial Crime Investigation can be found here: https://www.oecd.org/tax/crime/tax-crime-academy/

4 Monitoring, Evaluation, and Impact Measurement

The tax crime strategy will benefit from periodic review to ensure that the strategy is meeting its objectives and that actions to address the risks are having the desired effect. This will support early identification of challenges that need addressing as well as ensuring that the strategy evolves to take account of changing risks as well as opportunities provided by new technology tools in tackling tax crime.

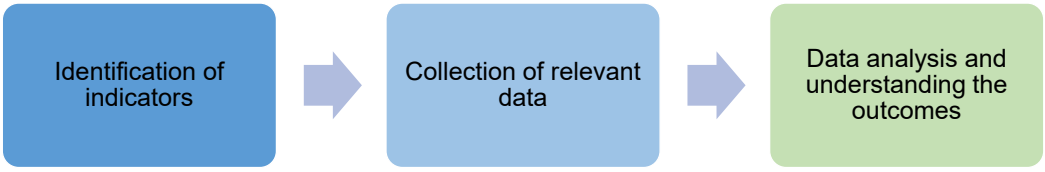
Throughout the implementation of the strategy, there will ideally be periodic internal reviews both within and outside the tax crime agency (including with policymakers) to assess the effectiveness of the strategy in achieving its goals and objectives. The exact way in which a jurisdiction does this will vary.

This matters not only for general reporting and accountability purposes regarding resource utilisation, but also aids in making necessary adjustments to the strategy, if required. This is important because it is likely that new threats will emerge or evolve, as well as new opportunities for tackling tax crime (such as new analytic tools or data exchanges) that the strategy will need to respond to.

Jurisdictions may wish to consider using specialist expertise to conduct, or at least guide, the evaluation process, whether in-house or external. Evaluation and measurement will often require a level of specialist skill. Independence from the function can also sometimes help to improve objectivity. In any event, evaluators should possess sufficient proximity to the strategy to be familiar with its detail and context, while collaborating with strategy leads in monitoring activities and gathering data.

The process for measuring the effectiveness of a tax crime strategy can be split into phases: (i) identification of indicators (ii) collection of relevant data (iii) data analysis and understanding the outcomes.

Figure 4.1. Process for measuring the effectiveness of the strategy



Source: Adapted from OECD Supporting SMEs to Get Tax Right: Strategic Planning (OECD, 2020[19])

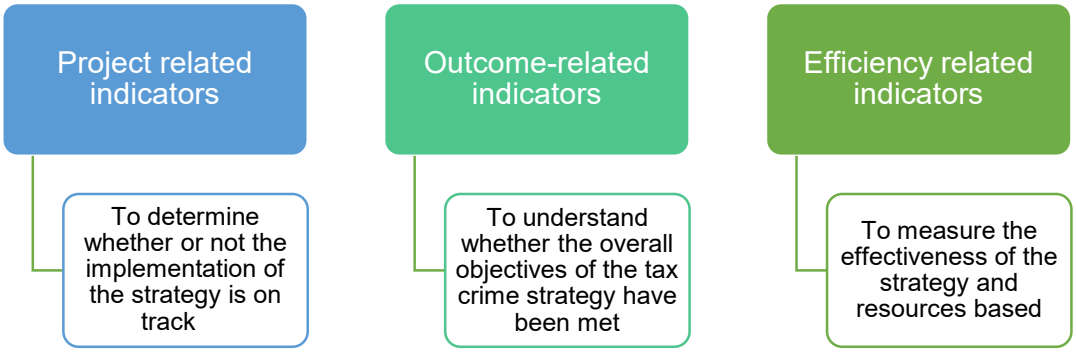
Identification of indicators

The strategy will set out a series of indicators that will assist jurisdictions in benchmarking the results of the strategy throughout its implementation (OECD, 2020[12]). These will depend on the action plan adopted, but should have a clear link to the objectives of the strategy. This may include comprehensive statistics on:

- The number of investigations, cases referred to prosecution, convictions, acquittals, and sentences and fines imposed.
- The number of cases where alternative sanctions were ordered, tax liabilities raised, and assets recovered.
- The number of investigations where plea agreements and settlements were secured prior to trial or conviction.
- The number of exchanges of information with both domestic and international partners, including through spontaneous, on-request and automatic exchanges.

It is likely that there will be different kinds of indicators that are wide-ranging, focusing on qualitative or quantitative metrics and supporting different phases of the strategy and its implementation.

Figure 4.2. Potential categories of indicators



Note: This is one example of the different categories of indicators that could be used to understand the effectiveness of the tax crime strategy.
Source: OECD

Box 4.1. Identification of indicators

Example from the United States

International Revenue Service - Criminal Investigation (IRS-CI) serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law. IRS-CI use various measures to evaluate performance that are related to the successful prosecution of criminals for committing various financial crimes, including tax evasion, money laundering, and violations of the Bank Secrecy Act.

Below is a performance chart published in the IRS-CI Annual Report in 2023, which provides examples of the various indicators used to measure and evaluate performance.

FY Combined Results

	2023	2022	2021
Investigations Initiated	2676	2558	2581
Prosecution Recommandations	1838	1837	1982
Informations/ Indictments	1676	1670	1856
Sentenced	1479	1490	1268
Incarceration Rate	79%	77%	78%
Average Months to Serve	48	42	43

Source: IRS-CI

Data collection

Once a set of indicators has been selected, it is necessary to collect the relevant data. While there are various ways of collecting data, each indicator may require a different approach. Box 2.4 in Chapter 2 lists some of the different sources of information that jurisdictions might want to draw on to collect the data.

Analysing the data and understanding the outcomes

The next step is to analyse the collected data and turn it into usable information. The collected information should then be compared to the base values established before the strategy was put into place.

Jurisdictions should use the results of the analysis to identify areas that might need adjustment and to understand the causes of the underlying issues. The results should be discussed with the relevant stakeholders who are dealing with this segment. For example, statistics on arrests would be discussed

with the police. The lessons learnt from the analysis and the discussions can then be used to update the existing strategy or to inform a new strategy.

Value for Money

The strategy should also be periodically reviewed to ensure it is achieving value for money. Officials working on the strategy will make sure to consider both cost estimates of tax crime and of investigating tax crime, when available. This will help measure the impact and effectiveness of the implementation of the strategy over time. It is expected that over the course of the implementation of the strategy, its value for money will be positive, i.e., that the strategy will help recover more money from tax crime than it made the government spend on detecting and investigating it. National statistics offices are usually best placed to provide estimates of the cost of tax crime, which can help to identify the scale of the wider impact of tax crime in the overall economy.

The wider revenue effects of the strategy may also be considered and measured as the result of behavioural change following government action. For example, in addition to the amount of money recovered, perhaps the strategy generated increased compliance in its targeted areas or yielded intelligence that identified other enablers or pursuable groups of taxpayers. In measuring this, there should be a clear causal connection between government activity and the change in taxpayer behaviour.

In addition to revenue effects, there may also be non-revenue related wider effects, such as increased trust in authorities as a result of seeing action against tax crimes.

Box 4.2. Value for money

Example from the United States

Each year, the Internal Revenue Service (IRS) sends a report to Congress justifying the agency's budget request. This report, titled "Congressional Budget Justification & Annual Performance Report and Plan" contains, among others, key operational data including performance results and achievements, previous budgets and priorities, and proposed budgets and justifications. This publicly available report provides two statistics for the Criminal Investigation Branch – Criminal Investigations Completed and Conviction Rate. Each year these statistics are compared against the target set at the beginning of the year.

Further, this report provides a Return on Investment (ROI) for IRS Major Enforcement Programmes which is calculated by dividing revenue by cost. The IRS has averaged an ROI from $5 to $9 over the past several years meaning that for every $1 spent on enforcement, the IRS collects $5 to $9 in tax, interest, and penalties. These figures do not take into account the deterrence effect of large civil and criminal tax enforcements on voluntary compliance.

An analysis performed by the Congressional Budget Office in response to a proposal to increase funding for the IRS by $80 billion over a 10-year period indicated revenues would increase by approximately $200 billion over the same period.

Source:
1. https://home.treasury.gov/about/budget-financial-reporting-planning-and-performance/budget-requestannual-performance-plan-and-reports/budget-documents-congressional-justification
2. https://www.cbo.gov/publication/57444#:~:text=CBO%20estimates%20that%20portions%20of,billion%20over%20those%2010%20years.

5 Case studies

A Case Study from the Internal Revenue Service - Chile

Context

Tackling tax evasion poses a fundamental challenge for any jurisdiction seeking to maintain the integrity of its financial system and promote fiscal equity. In this context, Chile has taken the approach of integrating its tax crime strategy with wider tax compliance work. The starting point is the Tax Compliance Management Plan (PGCT), an annual strategy that is complemented by an Integrated Tax Compliance Management Model (MIGCT). These are both aimed at ensuring tax compliance and reducing evasion through preventive measures.

Concerning tax crimes, once risks of tax non-compliance are identified, a series of specific actions are designed to address them through the strategy. Within this framework, the most aggressive tool is the prosecution of those who engage in tax crimes.

Tax Crime Risk Management

Risk management refers to the process of identifying, evaluating, and controlling the risks regarding non-compliance. To achieve this, the Chilean Revenue Service (SII) is comprehensive in the implementation of appropriate policies, processes, and controls to minimise risks and maximise opportunities. In the realm of identifying and analysing risks in tax crime matters, Chile has made progress in:

- The early detection of taxpayers with aggressive behaviour, reducing the possibility of fraud and erosion in the collection of Value Added Tax (VAT). In these cases, SII monitors the start-up process and life cycle of taxpayers, incorporating controls to trigger reviews when potential risks arise, as well as electronically restricting the issuance of tax documents to prevent fraud.
- Leveraging the available information in SII's databases to reinforce intelligence, designing and implementing business rules, and building analytical models to detect taxpayers according to risky behavioural patterns.
- The intensive use of analytical tools, which has strengthened detection in key areas with specific risks, such as: informal records, detection of fictitious losses, inaccurate declarations, anomalies in operational flows, traceability of relevant transactions, monitoring of high-value assets and refund requests.

Analysis is carried out by multi-disciplinary teams composed of data analysts, auditors, engineers, and lawyers, who interact with teams from regional offices to strengthen the analysis.

Targeted Action Plans

Within the MIGCT, specific action plans are deployed to address tax non-compliance. These plans focus on high-risk sectors and evasion patterns identified through risk analysis, alongside prosecution and

criminal actions when required. For example, SII has defined specific action plans, with target areas including the following:

- Taxpayers with high value assets
- Companies and their related entities that commit asset dilution and/or unreported international investments
- Cases of fake automotive companies selling stolen cars
- Improper VAT refunds for exports

For the action plans, there is co-ordinated work within the operational units in each SII office to review potentially evasive taxpayers and determine whether criminal action needs to be initiated. In such cases, SII presents the respective complaints or lawsuits to the competent authorities. The exercise of criminal action rests exclusively with the Director of SII.

Furthermore, faced with increased crimes in Chile linked to organised crime groups, SII has also included various initiatives in its strategy to combat this. For example, legislative projects to aid in the detection and prosecution of those who engage in organised crime have been introduced, in addition to working groups aimed at both identifying organised crime networks through the provision of information available in SII's databases, and to inform the Public Prosecutor's Office of the information gathered from tax audits, which may be related to tax crimes.

Whole of Government Approach

SII addresses crimes through a multi-disciplinary approach and has a series of agreements on collaboration with other government entities, highlighting co-operation with the Public Prosecutor's Office (Ministerio Público), Customs (Servicio Nacional de Aduanas), and the Financial Analysis Unit (UAF). This not only allows for the exchange of information, but also the pooling of resources, knowledge and skills to achieve common objectives more efficiently. By working collaboratively and in a coordinated manner, SII have seen significant improvements in the detection, analysis and prosecution of tax crimes, especially in larger and more complex cases.

Communicating the Tax Crime Strategy

Communication of the tax crime strategy focuses on informing the public about the risks involved in engaging in tax crime.

Press releases are made regarding lawsuits or focus areas of interest, and preventive communication campaigns are also conducted through social networks, mainly using platforms such as LinkedIn and Instagram.

Evaluating the Strategy

There are a series of performance indicators used to regularly evaluate progress towards established goals, so the strategies can be adjusted if necessary. These include the number of detected tax crime cases, the criminal lawsuits filed, and the results obtained in courts regarding tax crimes, as well as annual targets linked to the revenue obtained from reduced evasion and avoidance.

A Case Study from the Internal Revenue Service – Criminal Investigations – United States

The Internal Revenue Services' (IRS) success in the tax enforcement arena is heavily dependent on Criminal Investigation's (CI) ability to investigate and recommend prosecution of criminal tax violations to the Department of Justice. CI is the only federal law enforcement agency that can investigate and recommend prosecution of criminal tax violations. Publicizing these prosecutions provides a strong deterrent message to would-be tax evaders, ensuring the integrity and fairness in the tax system. Additionally, the intelligence gained in these tax investigations often allows CI to make significant contributions to other vital national priorities such as terrorism financing, Transnational Organized Crime (TOC) and HIDTA/OCDETF.

For CI to successfully contribute to IRS' overall goals in tax enforcement we must focus on our mission to "serve the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law." To accomplish this we must effectively select, develop, and investigate the most significant cases. We must continue prioritizing investments in data acquisition and technology to meet the emerging challenges of cyber enabled financial crimes, to address the prevalence and management of digital evidence and data, and to manage increasing data sharing and digitalization requirements. Additionally, to become more efficient and maximize the limited IRS resources devoted to our mission we must continue to develop all CI employees and collaborate internally and externally.

Considering these driving factors, the FY 2023 and 2024 priorities are divided into six areas:

- Case Selection
- Data and Technology
- Case Development and Investigation
- Communications
- Workforce Development
- Strategic Partnerships

Case Selection

Criminal Investigation Strategy: Focus case selection on high impact cases that maximize tax and tax-related financial crime deterrence by geographic coverage, industry, and issue.

IRS Strategic Goal:

- Protect the integrity of the tax system by encouraging compliance through administering and enforcing the tax code.

CI will emphasize high impact cases that focus on tax and related financial crimes to promote deterrence and generate significant sentences to discourage similar criminal violations by other taxpayers. Investigations will be conducted in three broad areas: traditional/core mission tax crimes, tax-related and other financial crimes, and narcotics related financial crimes. In addition, there will be an increased focus on crimes with an international nexus and collaboration with the IRS' National Fraud Program to enhance the fraud referrals from IRS business units. CI will continue to collaborate on multiple cross BOD endeavors with the Office of Fraud Enforcement and other IRS Business Operating Divisions to drive compliance.

Traditional/Core Mission Tax Crimes:

- **Abusive Tax Schemes**: Combat domestic and foreign abusive tax schemes. CI will identify and investigate tax scheme promoters as well as those who play an integral role in facilitating, aiding, or furthering abusive tax schemes.
- **Corporate Fraud**: Investigate criminal activities undertaken by business owners or companies that are designed to give an advantage to the perpetrating individual or company.
- **Employment Tax**: Place a high priority on attempts to evade or circumvent the duty to withhold, account for, and pay over employment taxes.
- **General Tax Fraud:** Significant resources will be devoted to traditional legal-income- source tax investigations involving individuals contributing to the tax gap by intentionally underreporting income, underpaying taxes due and repeated failure to file tax returns (Spies evasion), whether for themselves, family, business partners or legal entities they own or control.
- **International Tax Fraud**: Pursue a comprehensive international strategy to combat offshore tax crimes committed by individuals, corporations, and professional enablers. CI will continue to foster relationships and communication with foreign government officials, international financial institutions, regulators, and other external stakeholders to increase domestic prosecutions of those in non-compliance with the nation's tax laws. CI will explore and evaluate additional foreign posts to bolster overall tax compliance with a specific focus on additional cyber posts. In addition, CI will continue to work with foreign partners to build capacity through joint investigative activity, training, and outreach opportunities.
- **Joint Chiefs of Global Tax Enforcement (J5):** The J5, an alliance between the criminal tax authorities of the U.S., Australia, Canada, The Netherlands, and the United Kingdom, will continue to be a priority for CI and its Office of International Operations. The J5 is committed to combatting transnational tax crime through increased collaboration. CI will continue to collaborate with J5 partners to gather information, share intelligence, conduct operations, and build the capacity of tax crime enforcement officials. Working within existing tax treaties and laws, CI will focus on developing, initiating, and investigating cases with its J5 partners involving international tax evasion, professional enablers, virtual currency crimes, and other emerging fraud schemes.
- Questionable Refund, Return Preparer Fraud and Stolen Identity Refund Fraud: Investigate tax return preparers and others who promote schemes designed to obtain fraudulent refunds or to fraudulently reduce their clients' tax liabilities. Additional focus will remain on all refund fraud areas, including fictitious refundable credits and false filings. Field offices will continue to investigate significant Stolen Identity Refund Fraud (SIRF) schemes to enhance compliance and reduce the risk of identity theft. CI will enhance compliance and reduce the risk of fraud through outreach with the tax professional community, as well as our state and local law enforcement partners.

Tax Related and Other Financial Crimes:

- **Counterintelligence/Counterterrorism/Terrorist Financing:** Support national security efforts by providing financial expertise to the Joint Terrorism Task Forces, Counterintelligence Task Forces, Bank Secrecy Act (BSA) Review Teams and Financial Crimes Task Forces, and the worldwide pursuit of national security threats.
- **Cyber Crimes/Digital Assets:** Expand CI capabilities in response to the ongoing threat of cyber enabled data theft, refund fraud, and other virtual financial crimes. Cyber Crimes HQ section and the Cyber Crimes Units will collaborate with field office coordinators throughout the country to identify and pursue tax, identity theft, refund crimes, and money laundering in the cyber arena. More information can be found in CI's Cybercrime Strategy.

- **Money Laundering (non-narcotics):** Investigate complex and significant money laundering activity outside of the narcotics arena. CI has the distinct ability to follow illegal proceeds through a stream of legitimate commerce and financial institutions. More information can be found in CI's Money Laundering Strategy.
- **Public Corruption:** Pursue public corruption investigations, in collaboration with our law enforcement partners, where elected or government officials violate the public's trust.
- **Professional Enablers**: Together with the J5 Enablers Group, identify and investigate those who enable and facilitate offshore tax crime and money laundering to include promoters, offshore service providers and the offshore financial industry.
- **Emerging Threats:** In collaboration with our law enforcement partners, CI will focus our efforts to identify and pursue investigations on emerging threats of local, national, or international significance and against the most egregious offenders involved in the fraud. The focus on the emerging threats will foster the public's confidence in, and compliance with, the tax system.

Narcotics Related Financial Crimes

- Organized Crime Drug Enforcement Task Forces (OCDETF); Cyber-OCDETF; High Intensity Drug Trafficking Area (HIDTA); Transnational Organized Crime (TOC); Third Party Money Laundering (3PML); Trade Based Money Laundering (TBML): CI is committed to providing investigative resources and financial expertise to OCDETF investigations focused on disrupting and dismantling significant transnational criminal organizations (TCOs). These TCOs exploit and corrupt commercial business networks, financial institutions, and modes of international transportation while protecting their activities through a pattern of corruption and violence. Sophisticated TCOs are organized to take advantage of sovereign national borders to coordinate and operate illegal business ventures by exploiting privacy laws and the limitations of nations to investigate beyond their borders. These sophisticated TOC entities have created a need for experts in law, finance, communication, and technology to provide services that facilitate illicit financial flow. Those entities that offer their expertise and services to TOC entities have been labelled, third party money launders (3PML). CI will continue to provide investigative resources towards the pursuit of criminal charges against significant narcotics organizations, darknet vendors and administrators, 3PMLs and TCOs while incorporating all applicable asset forfeiture provisions to deprive these illicit networks of their profit motive.

Strategic Application of Resources

- Consistent with these priorities and based upon the success of recent Service-wide fraud prevention programs, CI will continue to strategically balance its nationwide resources devoted to Identity Theft (IDT), Questionable Refund Program (QRP), and Return Preparer Program (RPP) fraud to help maximize the percentage of resources devoted to the development and investigation of traditional tax cases.
- We will continue to minimize investigations which do not require our financial investigative expertise, where the primary violations fall within the purview of one or more other agencies, and where only minimal support to our traditional tax mission is provided. Additionally, we will scrutinize our participation in investigations with violations that are likely to result in minimal sentences, such as misdemeanors. **All case initiations concerning misdemeanors, mortgage fraud, Ponzi schemes, gaming, embezzlement, or violations of Title 18 USC §§ 2 (aiding and abetting), 1349 (attempt and conspiracy), and 1960 (unlicensed money transmitter), will continue to require Director, Field Operations approval.** We recognize there are impactful investigations that fall in these categories, to include high dollar, complex and high notoriety investigations and these factors will be given additional consideration in the case selection process.

Case Development and Investigation

Criminal Investigation Strategy: Incorporate a team-based approach to case development, providing tools and support necessary to effectively investigate cases.

IRS Strategic Goals:

- Protect the integrity of the tax system by encouraging compliance through administering and enforcing the tax code.
- Advance data access, usability, and analytics to inform decision making and improve operational outcomes.
- Drive increased agility, efficiency, effectiveness, and security in IRS operations.

CI will incorporate a team-based approach to enhance the effectiveness and efficiency of case development and investigations by providing the necessary tools and support. CI will use data to drive decisions on case selection and technology to identify patterns of non-compliance and potential cases within those patterns.

Each case should have significant potential for incarceration, publicity, and broad impact in furtherance of our mission to deter would-be criminals and demonstrate to the law abiding public that their tax dollars are applied purposefully and responsibly.

The Nationally Coordinated Investigations Unit (NCIU) will continue to identify high-impact, mission focused, and multi-jurisdictional investigations by leveraging partnerships and utilizing data analytics to identify significant non-compliance areas and emerging threats to tax enforcement. The NCIU will integrate case agents, investigative analysts, data scientists, and prosecutorial resources to generate and support mission driven investigations relating to national initiatives.

Field offices will collaborate with CI Headquarters to request specific data sets from civil Business Operating Divisions for local case development initiatives in furtherance of CI's team-based approach to case development. Successful case development ideas should also be shared with the DFOs, the NCIU, Applied Analytics and others to avoid duplication of effort and to maximize use of productive case development strategies. Case development initiatives by the NCIU and Applied Analytics will continue to be governed by the CI Executive Steering Committee or other executive oversight process to provide transparency and reduce the risk of duplication. CI will take a leading role on enterprise wide data driven enforcement initiatives.

Workforce Development

Criminal Investigation **Strategy**: Cultivate and advance a distinct, diverse, and inclusive culture that values and maximizes the talent, skills, and experience of the CI workforce and provides career development and advancement opportunities for all employees at every level of the organization.

IRS Strategic Goals:

- Educate, advocate, engage and empower the CI workforce by cultivating partnerships and resources to create and sustain an environment that is inclusive, equitable and diverse.
- Identify, attract, and retain a pipeline of diverse and highly qualified candidates with a wealth of experience and talent through targeted outreach, recruitment, and selection.
- Advance data access, usability, and analytics to inform decision making and improve operational outcomes.
- Ensure leadership demonstrates its commitment and accountability for modeling behaviors that advance diversity, inclusion, and accessibility.

CI will enhance workforce development by hiring and training new special agents and professional staff, by developing a workforce that values collaboration and inclusion. CI will utilize best practices and strategies to recognize and retain our diverse workforce while employing professional career development and advancement opportunities that will lead to a more engaged workforce where employees feel valued and are inclined to stay. Having an organization with diverse employees at every level helps strengthen CI and makes it an open, safe place that breeds new ideas and innovation. Extensive EDI training will augment CI promoting the ideals of creating a respectful and safe work environment while advancing inclusive leadership skills throughout our entire management cadre. Along these efforts, CI will continue to evolve by re-evaluating its organizational structure to ensure it best aligns human capital with our investigative priorities that best positions CI for the future.

- **Engaging All Employees:** CI leaders will emphasize the value of belonging and the work contributions made by employees while taking an integrated approach that focuses on improving and communicating expectations, retention strategies, and measures of teamwork effectiveness, which impacts our metrics in employee engagement.
- **Improve Employee Satisfaction**: CI will use transparent communication and employee recognition programs to make the IRS the best place to work in the federal government. We will engage all employees through the Federal Employee Viewpoint Survey, the Ask the Execs Program, and the IRS Employee Suggestion Program. Additionally, we will recognize employee contributions through various channels, including the IRS and Chief's Recognition Programs.
- **Professional Staff Utilization and Effectiveness:** CI will continue to develop and utilize clearly defined career paths for professional staff to maximize advancement opportunities. The "investigative professional staff" groups are now a permanent structure in CI and are fully operational in every CI field office. CI will continue to find more effective ways to utilize non-investigative professional staff to support operations in a way that improves efficiencies and capitalizes on the skills and abilities of administrative staff at all levels of the organization.
- **Hiring and Development of New Special Agents:** CI will continue seeking to secure funding to hire and develop additional special agents, strategically aligning future hiring with the greatest business needs in specified field offices.
- **Training and Development Opportunities**: CI will support training opportunities for all employees as funding is available. CI will also support no-cost training when available and appropriate. Under the leadership of CI's Workforce Development organization, CI will identify and develop future leaders using the Leadership Succession Review (LSR) process or successor process, and by delivering a holistic leadership development program that covers all employees from the time they enter CI through advancement to senior leadership positions.

Data and Technology

Criminal Investigation **Strategy:** Integrate ever-evolving and employee focused technologies that drive a more agile, efficient, mobile, and impactful financial investigative capability.

IRS Strategic Goals:

- Advance data access, usability, and analytics to inform decision making and improve operational outcomes.
- Drive increased agility, efficiency, effectiveness, and security in IRS operations.

CI will identify, evaluate, test, and deploy new technologies that empower its employees to become more efficient, effective, collaborative, and mobile with their investigative capabilities. CI will prioritize investments in data acquisition and technology that are focused on meeting the emerging challenges of cyber enabled financial crimes, the prevalence and management of digital evidence and data, and increasing data sharing and digitalization requirements. In addition, CI will leverage cost effective

alternatives for commodity type technology services, such as open-source tools, while focusing limited resources on technologies uniquely geared to meet law enforcement requirements. CI continues to invest in collaborative ventures and technologies focused on improving investigative deconfliction abilities, investigative efficiencies, and data sharing capabilities in an overall effort to enhance relationships with other law enforcement agencies while remaining compliant with agency data sharing policies. CI will create and implement a data governance policy that will allow both a more robust review of documents and drive efficiencies throughout the investigative process. CI's Applied Analytics organization will spearhead the use of modern analytical techniques, such as artificial intelligence, process automation, and others, to integrate available data into an investigative computing platform to assist CI's law enforcement agents in identifying criminals and bringing them to justice as quickly as possible.

Communications

Criminal Investigation **Strategy**: Integrate innovative channels and proactive communication strategies to effectively communicate as a law enforcement agency and promote deterrence.

IRS Strategic Goals:

- Empower and enable all taxpayers to meet their tax obligations.
- Protect the integrity of the tax system by encouraging compliance through administering and enforcing the tax code.
- Collaborate with external partners proactively to improve tax administration.

CI will maximize the impact of criminal enforcement and encourage voluntary compliance through publicity, education, and outreach. Publicity will focus on informing the public about CI enforcement efforts and educating the public about various fraud schemes and scams they should avoid in areas such as tax related identity theft or other emerging or prevalent schemes.

CI will integrate innovative channels and proactive communication strategies to effectively communicate as a law enforcement agency and promote deterrence of financial crime and increase our visibility as an organization. CI will continue exploring ways to develop a presence on social media outlets to distribute information and help foster voluntary compliance.

Collaboration with external stakeholders and broad outreach efforts are paramount to educating our partners regarding CI's positive impact locally, nationally, and worldwide. We will strengthen relationships with the tax professional community, local, state, and federal government partners, the private sector, as well as financial institutions. CI will also lead and participate in local and regional bank forums, engage academia, and will continue to educate lawmakers about the relevance, successes, and abilities of CI through various channels to include in-person briefings, press releases sent to member offices, and coordinated constituent presentations.

Strategic Partnerships

Criminal Investigation Strategy: Foster strategic partnerships to enable greater resource efficiency and cultivate strong CI advocates across IRS, law enforcement, and Congress.

IRS Strategic Goals:

- Protect the integrity of the tax system by encouraging compliance through administering and enforcing the tax code.
- Collaborate with external partners proactively to improve tax administration.
- Drive increased agility, efficiency, effectiveness, and security in IRS operations.

CI executives and senior leaders will focus on strengthening partnerships with internal and external stakeholders to advance shared interests and generate advocacy by improving communication and transparency, developing employees' skills, enhancing CI's organizational structure, continuing a focus on risk management and engaging with employees to improve operations at all levels within CI.

- **Improve Internal Communication and Transparency**: Clear and frequent communication will be used to deliver organizational goals and expectations and will encourage employees to elevate ideas and issues through all levels of management. CI will continue to review our organizational structure to ensure we are aligned and focused on maximizing the impact of available resources.
- **Improve Collaboration within IRS:** CI executives and senior managers will seek opportunities to collaborate within IRS to improve tax enforcement through initiatives and programs throughout the Service which align with our law enforcement priorities. We will explore processes and technologies utilized in other parts of the Service which may improve the efficiency of our current operations, as well as share CI best practices, to timely identify patterns of non-compliance, determine the proper enforcement method and deliver high impact cases which foster compliance with tax law.
- **Advance Communication, Coordination and Collaboration with External Stakeholders and Department of Treasury**: CI executives and senior leaders will continue to develop strong working relationships through persistent contact with the DOJ and US Attorney Offices and will leverage relationships developed and held by the Treasury, Legislative Affairs, TEOAF, and FinCEN liaisons. These efforts should result in an increase in prosecutions of those in non-compliance with the nation's tax laws. Senior leaders should develop and expand relationships with key members of the tax professional community, to include financial institutions, associations, international strategic partners, and tax professionals. Additionally, senior leaders will develop and maintain working relationships with education institutions and other public/private industries as appropriate.

"Honor the badge, Preserve the legacy, Master your craft, and Inspire the future"

A case study from His Majesty's Revenue & Customs – United Kingdom

Overview

HMRC (HM Revenue & Customs) is the sole operational department responsible for tackling fiscal fraud and Serious Organised Crime attacks on the UK tax system. HMRC is funded by His Majesty's Treasury and has a vital duty to ensure it operates a fair tax system, while tackling those that deliberately and dishonestly set out to defraud HMRC – to make sure that those who try to cheat the Exchequer, through whatever means, are identified and forced to pay what they owe.

While the majority of people abide by the law and pay their taxes, there are those who deliberately and dishonestly set out to defraud HMRC by evading tax, stealing public funds, or cheating the system in other ways. Tax fraud undermines our economy, creates unfair competition for legitimate businesses and robs our vital public services of much-needed funds. It also supports other crimes that harm our communities.

By bearing down on tax fraud HMRC builds public trust: honest taxpayers, rightly, want to know that HMRC will step in to enforce the rules where necessary, creating a level playing field for individuals and businesses.

What is tax fraud?

HMRC defines fraud as any deliberate omission, concealment, or misinterpretation of information, or the false or deceptive presentation of information or circumstances in order to gain a tax advantage.

Tax fraud covers a wide range of illegal activity, including:

deliberately submitting false tax returns

falsely claiming repayments or reliefs

hiding income, gains, or wealth offshore

smuggling taxable goods

Some of this is carried out by dishonest individuals but organised criminals also deliberately target the tax system for financial gain.

HMRC's approach

The best way to tackle tax fraud is to stop it happening in the first place. HMRC does this by:

building checks and controls into its systems;

changing legislation to make it more difficult or impossible to commit tax fraud;

working with businesses to help them spot when they are at risk of tax fraud.

When tax fraud does happen

When tax fraud does happen, HMRC has a range of powers and specialist investigation capabilities that enable them to uncover even the most complex and determined frauds and bring the perpetrators to account.

Most of HMRC's work to tackle tax fraud makes use of its civil powers. These allow HMRC to get hold of the information it needs to identify and collect unpaid tax, while imposing financial penalties on those responsible (up to 200 percent of the tax due in some cases).

In some serious cases of tax fraud, HMRC can use the approach set out in its Code of Practice 9 (https://www.gov.uk/government/publications/code-of-practice-9-where-hm-revenue-and-customs-suspect-fraud-cop-9-2012): in exchange for individuals admitting their dishonesty, paying all their tax and significant financial penalties, they won't face a criminal investigation, which otherwise could be the case.

Criminal Investigations

While HMRC reserves complete discretion to conduct a criminal investigation in any case, its approach is to use its criminal and specialist investigation capabilities in certain circumstances.

Firstly, when a fraud is particularly serious. For example, those involving large losses or where the conduct or individuals involved merit a strong response, such as HMRC's work to tackle organised crime groups.

Secondly, when HMRC wants to send a strong deterrent message that reassures the honest majority there is a level playing field. That could be tackling a particular type of fraud, or targeting specific business sectors or customer groups where we know tax fraud is prevalent. HMRC's work to tackle promoters of fraudulent tax schemes and those professionals who carry out or enable tax fraud is evidence of this. HMRC is clear that the tax rules apply the same to everyone, regardless of wealth, profession, or resources.

And thirdly, when HMRC's civil powers aren't enough to uncover the truth or recover the tax that is at stake. This includes the use of HMRC's covert capabilities to unmask the workings of organised criminals or its more coercive powers, such as searches and arrests.

These are significant powers and are rightly subject to rigorous external oversight and safeguards, like other law enforcement agencies.

Criminal cases can be expensive and time consuming, so it's only right that HMRC uses them selectively to ensure they deliver both value for money for the taxpayer and the maximum impact on tax fraud. In recent years, HMRC has deliberately focussed them on the most harmful, complex, and sophisticated frauds.

It's an approach that's about reaching the right outcome for the UK, rather than chasing arbitrary targets for arrests and prosecutions.

Collecting what is owed

Whatever approach we take, HMRC always seeks to recover the money owed.

Where possible, that's through issuing tax assessments or reaching agreements with taxpayers for the full amount of tax owed, applying penalties and interest as appropriate. These are often sufficient to recover monies owed. When HMRC needs to go further, it have access to a raft of other powers that allow it to disrupt and recover the proceeds of tax fraud.

That includes those under the Proceeds of Crime Act, which enables HMRC to identify, confiscate and sell the assets of those convicted of tax fraud. Failure to comply with these confiscation orders can lead to more jail time for the perpetrators.

Account Freezing Orders, meanwhile, allow HMRC to quickly and effectively freeze and forfeit money in suspect bank accounts, stopping fraudsters from transferring funds out of our reach. HMRC also continues to seize physical amounts of cash as part of its work.

And where HMRC needs to tackle companies involved in tax fraud, it can, and does, work with financial institutions and liquidators to wind them up, identifying and seizing their assets in the process.

These are unrivalled asset recovery powers that send a message that tax fraud does not pay.

Tackling enablers of tax fraud

Tax fraud is becoming increasingly sophisticated and complex, with those involved requiring the services of professional enablers to help them transfer wealth anonymously or launder the proceeds of crime.

HMRC is determined that these enablers should face the consequences as much as those they help to carry out tax fraud.

That includes using the Corporate Criminal Offence (CCO) to root out wrongdoing across business sectors. The CCO has made it a criminal offence if an organisation fails to stop those acting on its behalf from facilitating tax fraud. With potentially unlimited fines for organisations found guilty, the CCO is not just about corporate prosecutions but about changing industry practice and attitudes towards risk, encouraging businesses to do more to prevent tax crime happening in the first place. HMRC is already seeing positive signs that this is happening.

Working with partners

While HMRC is the single UK organisation with responsibility for tackling tax fraud, it works alongside a range of partners, including financial institutions, professional bodies, other government departments and law enforcement agencies and international tax and customs authorities.

For example, HMRC is a founding member of the Joint Chiefs of Global Tax Enforcement (J5) – an operational alliance between the UK, Canada, the US, Australia, and the Netherlands, dedicated to tackling international tax crime, money laundering and those who enable it. The J5 is currently working on a significant number of investigations, including cases involving influential international enablers of tax fraud.

It is partnerships like these that allow HMRC to track down and return those criminals who believe they can flee justice by going overseas, including some of the UK's most harmful tax cheats.

Reporting tax fraud

Tax fraud is an issue for us all because it takes from us all. Whether that's the money it steals from our vital public services or the harm that organised criminals cause to our communities, we all have a responsibility to tackle it.

HMRC have an online reporting tool (report it online) and a Fraud Hotline (Fraud Hotline on 0800 788 887 for anyone with information about tax fraud to report to.

References

FATF (2013), *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment*, FATF. [8]

FATF (2012-2023), *International Standards on Combatting Money Laundering and Financing of Terrorism & Proliferation*, FATF, http://www.fatf-gafi.org/recommendations.html. [7]

Internal Revenue Service (2023), *Internal Revenue Manual*. [11]

OECD (2024), "Recommendation of the Council to Facilitate Co-operation between Tax and Other Law Enforcement Authorities to Combat Serious Crimes". [9]

OECD (2023), *Communication and Engagement with SMEs*. [18]

OECD (2023), "Comparative Information on OECD and other Advanced and Emerging Economies". [2]

OECD (2023), "Dividend Tax Fraud: Raising Awareness of Dividend Stripping Schemes". [4]

OECD (2023), *Enhancing Inter-Agency Trust Between Tax and Other Financial Crime Authorities*. [17]

OECD (2023), *Facilitating the Use of Tax-Treaty Exchanged Information for Non-Tax Purposes: A contribution to the whole-of-government approach to tackling illicit financial flows*, OECD, https://www.oecd.org/tax/transparency/documents/facilitating-the-use-of-treaty-exchanged-tax-information-for-non-tax-purposes.pdf. [22]

OECD (2022), *Crypto Assets Reporting Framework and Ammendments to the Common Reporting Standard*, OECD Publishing, https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm. [21]

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, https://doi.org/10.1787/006a6512-en. [13]

OECD (2020), "Tax Administration 3.0: The Digital Transformation of Tax Administration". [6]

OECD (2020), *Tax Administration: Supporting SMEs to Get Tax Right Series: Strategic Planning*. [19]

OECD (2020), *Tax Crime Investigation Maturity Model*, OECD Publishing, https://www.oecd.org/tax/crime/tax-crime-investigation-maturity-model.htm. [12]

OECD (2019), *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, OECD Publishing. [24]

OECD (2019), *Tax Morale: What Drives People and Businesses to Pay Tax?*, OECD Publishing, Paris, https://doi.org/10.1787/f3d8ea10-en. [20]

OECD (2017), *Effective Inter-Agency Co-operation in Fighting Tax Crime and Other Financial Crimes - Third Edition*, OECD Publishing, https://www.oecd.org/tax/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-and-other-financial-crimes.htm. [14]

OECD (2017), *Fighting Tax Crime: The Ten Global Principles*, https://doi.org/10.1787/63530. [25]

OECD (2017), "Technology Tools to Tackle Tax Evasion and Tax Fraud". [5]

OECD (2013), *Bribery and Corruption Awareness Handbook for Tax Examiners and Tax Auditors*, OECD Publishing. [10]

Russell, B. (2010), *Revenue Administration: Developing a Taxpayer Compliance Program*. [26]

United Nations Office on Drugs and Crime (2011), "2011", *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*. [3]

UNODC (2010), *Guidance on the preparation and use of organized crime threat asssesments ("The SOCTA Handbook")*, United Nations. [16]

World Bank and OECD (2018), "Improving Co-operation between Tax Authorities and Anti-Corruption in Combating Tax Crime and Corruption". [15]

Yikona, S. et al. (2011), *Ill-Gotten Money and the Economy*, World Bank, https://doi.org/10.1596/978-0-8213-8887-7. [23]

Designing a National Strategy against Tax Crime

CORE ELEMENTS AND CONSIDERATIONS

Tax crimes negatively affect all countries, developed and developing alike. They obstruct governments' ability to collect revenue and undermine trust in the legal and financial system which can lead to a wide range of adverse outcomes. Tax crime is often closely linked to other forms of serious domestic and transnational crime, such as money laundering, corruption, the trafficking of drugs or people, and terrorist financing.

This report sets out the rationale for adopting a national strategy for countering tax crime and to support jurisdictions' efforts in designing such strategies, drawing from the practices of members of the OECD's Task Force on Tax Crimes and other Crimes (TFTC).

PDF ISBN 978-92-64-60508-4