PRO
TAX

Risk assessment framework for countering tax crimes

This publication has been produced with the financial support of the European Union's H2020 research and innovation programme under grant agreement No 787098.

The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Please cite this report as:

PROTAX (2021). *Risk assessment framework for countering tax crimes*. 787098 PROTAX EU H2020 Project.

Table of Contents

List of acronyms/abbreviations

Abbreviation	Explanation
AML	Anti-Money Laundering
CDD	Client Due Diligence
DPA	Deferred Prosecution Agreement
ETCB	Estonian Tax and Customs Board
EU	European Union
FIU	Financial Intelligence Unit
LEAs	Law Enforcement Agencies
KYC	Know Your Customer
OECD	Organisation for Economic Cooperation and Development
PRORAM	PROTAX risk assessment methodology
RPN	Risk Priority Number
WP	Work package

Executive summary

The PROTAX risk assessment methodology (PRORAM) is a tool that is specific to tax crimes and aims to provide practitioners with a model of how to self-assess suspicious behaviours and warning signs indicating a tax crime, together with a practical model for tax authorities, policymakers and other stakeholders to assess the risks and controlling tax crimes in their jurisdiction, and across the EU.

It is designed to offer practical support for policymakers and experts as well as serving as a training tool for enablers and professionals with reporting duties. It can also be used as a tool to build knowledge of threats, vulnerabilities and risks across the EU tax crime law enforcement ecosystem by bringing stakeholders together to work through the risks inherent to that environment.

Feedback on PRORAM's use and utility has been sought from stakeholders in relation to its effectiveness as an instrument for minimising tax crime risks during the WP7 co-creation workshop. Additional efforts have been conducted online to co-create this risk assessment methodology with partners in the consortium and other stakeholders. PROTAX will now promulgate its use through its contacts more widely in the context of its efforts in WP8.

This document details the risk assessment approach adopted by PROTAX, justifies and explains the use of the risk assessment methodology chosen, provides examples of it working, outlines use cases to

understand how it can add value within and across the EU, and finally, in the annexes, presents a series of risk tables to actually conduct risk assessments.

Introduction

National and regional risk assessment frameworks are currently being developed by the major international institutions concerned with tax and financial flows such as the World Bank[1], OECD[2] and Tax Justice Network (TJN).[3] No such risk assessment framework exists at an EU level yet and PROTAX will add value by providing one. PROTAX has identified through extensive work in WPs 1 – 6 that there are some important vulnerabilities internal to the EU's tax crime law enforcement environment that create challenges to successfully investigating and prosecuting tax crime. This risk assessment framework aligns with these key challenges, such as discrepancies in typologies of tax crime and different thresholds for tax crime and whistle-blower treatment. The focus of this risk assessment is to enable the user to identify such vulnerabilities in tax crime policy, law and institutional frameworks within and across EU jurisdictions and model them as risk. In doing so, users will be able to address risks to the tax system on the EU in a more optimum way. To do this in a way that is valuable for end users, faithful to the grant agreement and relevant to the key challenges of the project, this is a two-level risk assessment methodology.

The first level is a list of questions co-created with LEA partners that are pertinent to identifying suspicious behaviours that may indicate a tax crime. This first level can be considered as a KYC (Know Your Client) risk assessment for enablers on its own or can be used as a training or knowledge building tool. This first level serves to identify red flag behaviour that can then feed into, and be assessed by, the Failure Modes Effects Analysis (FMEA) risk methodology (which will be explained in detail below) developed by PROTAX. This level should, where appropriate, be used in conjunction with the second level.

The second level uses FMEA to identify the risks to controlling the red flags and suspicious behaviours identified in the first level. These risks refer to the likelihood and severity that certain institutional and legal vulnerabilities of the EU undermine the control of risks produced by certain suspicious behaviours. The second level can be used by policymakers and tax authorities to identify what those legal, institutional and cultural vulnerabilities in the tax crime ecology of the EU are. **Use cases** are outlined in section 3 that envisage use of the risk methodology to add value. This second level is an

[1] World Bank, 'Risk Assessment Support for Money Laundering/Terrorist Financing', 2016; https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support.

[2] The OECD 'Maturity Model' on tax crime investigations is yet to be published. However, discussions on its approach have taken place with a senior tax crime advisor from the OECD), who is also on the PROTAX stakeholder board. The Maturity Model is a way for countries to assess the stage at which their tax crime law enforcement environment – legally, institutionally and operationally – is 'mature' by international standards. However, there are other 'maturity models' by the OECD involving tax matters, such as: OECD, Technologies for Better Tax Administration: A Practical Guide for Revenue Bodies, 2016, https://read.oecd-ilibrary.org/taxation/technologies-for-better-tax-administration_9789264256439-en#page3 ; and, OECD, Tax Compliance Burden Maturity Model, OECD Tax Administration Maturity Model Series, 2019 Paris. www.oecd.org/tax/forum-on-tax-administration/publications-and-products/tax-compliance-burden-maturity-model.htm.

[3] Tax Justice Network (TJN), 'Financial secrecy index', 2020. https://fsi.taxjustice.net/en/ .

EU-wide risk assessment framework that aims to identify vulnerabilities and risks inherent to the EU tax crime law enforcement eco-system.

In order for both risk assessment methodologies to be usefully predictive of risk, they must have sufficient and relevant data. There are four sources for such data: the extensive work conducted in WPs 1 – 6, partner knowledge gained in the co-creation sessions, feedback from demonstrations to expert stakeholders as part of WP8, and end users interacting with the risk methodology in their professional decision making or as part of collaborative knowledge building exercises and training.

The rest of the document is structured as follows:

1. PROTAX risk assessment methodology (PRORAM): Explanation, process and principles outlines the way tax crime risk is addressed in this risk methodology, distinguishing between *threats* and *vulnerabilities*, and how they interact to increase the risk of both tax crimes being committed and unsuccessfully investigated and prosecuted. These vulnerabilities relate to the key institutional, legal and cultural factors identified in PROTAX WPs 1 – 6. This section describes and conceptualises the *risk assessment process* and the principles that guide PRORAM are set out.

2. Risk assessment level 1 and 2 provides background to the two levels of the risk assessment process adopted. Section 2.1. KYC risk assessment (level 1) describes common Know Your Client (KYC) approaches to identifying red flag behaviour in customers and clients and explains how PROTAX will include a similar approach in the risk methodology developed in this document. Section 2.2 discusses the EU-wide risk assessment framework method by which risk is assessed, including vulnerabilities identified in the findings of PROTAX WPs 1 – 6. It also discusses how this risk assessment methodology can create impact and contribute towards EU harmonisation on a number of legal, institutional and cultural levels.

3. Use cases. The four use cases in this section outline how PROTAX envisages the use of this risk assessment methodology, and how in each case it can add value and have impact. The use cases are:

- **3.1. Training for enablers:** This use case explains how PRORAM can be used as a training tool for enabler organisations and professionals with reporting duties.
- **3.2. Knowledge building at MS level**: This use case details how using PRORAM in knowledge building exercises or workshops within one Member State (MS) involving a variety of stakeholders (LEAs, tax authorities, policymakers, enablers) could add value to the MS and EU.
- **3.3. Knowledge building at EU level:** This use case explains the process by which knowledge building exercises or workshops could be conducted at an EU-level involving stakeholders from different EU organisations and MS. This is in order to work through the risk assessment methodology and seek areas where harmonisation can 'design out' key vulnerabilities at an EU-level.
- **3.4. Policymaking:** This use case explains how PRORAM can impact policymaking. In conjunction with the policy toolkit (D7.1), policymakers can work through the risk

methodology with LEAs and tax authorities in order to brainstorm and discover which specific policies could lessen the vulnerabilities identified in the risk methodology.

4. PROTAX risk assessment methodology (PRORAM): Failure Modes Effects Analysis (FMEA) explains in detail and justifies the use of the specific risk methodology that PROTAX has chosen and adapted for use and sets out guidance for the end user.

4.1 How it works: FMEA risk assessment methodology examples – this section sets out two example scenarios.

- First, a simplified example demonstrating how inputted data can produce risk priority scores, and how this can be evaluated using information gained in WP 1 – 6 is set out.
- Second, a more extensive example of how whistle-blower treatment can be evaluated to assign risk in more detailed uses of PRORAM.

Section **5. Final remarks** re-emphasises the contexts in which this risk assessment methodology can be used to create value and add impact and outlines how development of the risk assessment methodology will continue in WP8.

Finally, **6. Annexes** contains the tables and information required to conduct a risk assessment.

Annex 1a - Risk impact assessment of *suspicious transactions* is a risk assessment table assessing severity of red flag risks. **Annex 1b - Risk impact assessment of *control measures*** is a risk assessment table assessing severity of control risks. Severity is assessed in both cases by calculating likelihood and impact. **Annex 1c - Evaluation scheme for *control measures*** is a control evaluation table allowing users to quantify and assess the effectiveness of current control measures. **Annex 2 - Risk tables (vulnerabilities)** is a series of FMEA risk assessment tables with data inputted from PROTAX WP 1 – 6, which is the substantive core of the risk assessment methodology. **Annex 3 – Questions indicating suspicious behaviours or transactions or financial arrangements (red flags)** is a list of questions developed in conjunction with LEA partners to alert the user to a red flag that may indicate a tax crime. Finally, **Annex 4** - **Blank risk assessment tables** contains two blank FMEA risk assessment tables (**Annex 4a – risk assessment table for level 1** and **Annex 4b – risk assessment table for level 2**) that can be printed off and used in workshops and training events.

1. PROTAX risk assessment methodology (PRORAM): Explanation, process and principles

1.1 Risk assessment explanation

The ISO defines risk as the effect that uncertainties have on achieving objectives.[4] The purpose of risk assessment and management is to increase value insofar as it improves organisational performance and contributes to the achievement of objectives by identifying and mitigating against uncertainties.

The ambition for PRORAM is to develop and offer a process to coherently identify and analyse the uncertainties that are produced by threats and vulnerabilities in the tax crime law enforcement environment in the EU, by modelling these as risks. This will support the development of co-ordinated activities and measures to control them at an institutional and organisational level. This is also in line with the EU's view of the nature of 'vulnerabilities' and 'threats' set out in a different context to this risk methodology, which the 'Methodology for identifying high-risk third countries under Directive (EU) 2015/849' document.[5]

Threats – Threats are persons, groups, organisations or activities with the potential to cause harm to the financial system or economy of the EU. In the context of tax crime, this includes tax criminals, terrorist groups, facilitators and enablers. Threats serve as a starting point for understanding risk and this is the approach taken in PRORAM in level one, which identifies suspicious transactions and activities that may indicate a tax crime of some kind. The threat level is contingent on the capability to enact the threat. In the case of PRORAM, threat capability is not assessed on the basis of the capacities of an actual adversary, but rather, the extent to which key vulnerabilities and weaknesses contribute to the likelihood that a given threat could be enacted.[6]

Vulnerabilities - Vulnerabilities are 'those things that can be exploited by the threat or that may support or facilitate its activities'.[7] In the tax crime risk assessment context, vulnerabilities (as distinct from threats) are weaknesses in the anti-tax crime systems, controls and institutional features of a country.[8] Vulnerabilities could also include particular features of a financial product, sector or service that makes them more attractive to tax criminals. PRORAM particularly focuses on the vulnerabilities posed by the particular institutional and legal factors of the EU and MS.

Risk assessment – It is important to distinguish between threats, vulnerabilities and risks. Threats are a function of capability and harmful intent, vulnerabilities are the weaknesses that increase the capability of the threat. A risk refers to the likelihood that those threats will materialise and the consequent harm associated with such risks.[9] Risk assessment in this document, therefore, is the process of assessing the likelihood that tax crime threats materialise by assessing the extent to which

[4] Sandrine Tranchard, ISO, 'The new ISO 3100 keeps risk management simple', 15.02.2018. https://www.iso.org/news/ref2263.html

[5] European Commission, Methodology for identifying high-risk third countries under Directive. Commission staff working document, (EU) 2015/849, Brussels, 7.5.2020.

[6] Financial Action Task Force (FATF), 'National Money Laundering and Terrorist Financing Risk Assessment', Paris, 2013 [p7], https://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf .

[7] *Ibid.*

[8] European Commission, Methodology for identifying high-risk third countries under Directive. Commission staff working document (EU) 2015/849, Brussels, 7.5.2020

[9] Strachan-Morris, D., 'Threat and Risk: What is the Difference and Why Does It Matter?', *Intelligence and National Security*, Vol. 27, No. 2, 2012, pp. 172-186.

vulnerabilities in anti-tax crime systems or controls can be exploited by a threat. By assessing risk in this way PRORAM seeks to identify institutional and legal vulnerabilities in the tax crime law enforcement environment in order to 'design out' those vulnerabilities where possible, which will mitigate the risks posed by tax crime in the EU. The method adopted to do this is a Failure Modes Effects Analysis (FMEA), which is covered in detail in section 4.1.

Work conducted during PROTAX WPs 1 – 6 in focus groups, case studies and comparative legal analysis pointed to tax crime threats – meaning the risk of nefarious actors committing tax crimes are high – and vulnerabilities, particularly, weaknesses in the enforcement of tax crime law.

Where vulnerabilities occur
Scope and definitions of tax crimes
Threshold of tax crimes
Sanctions for tax crimes
Legal liability for tax crimes
International cooperation on criminal matters
Information sharing
Whistle-blower treatment
Obligations to report suspicious financial behaviour
Obligations to maintain secrecy of client's financial transactions (transparency versus secrecy)
Resource constraints

Decision-making in this environment carries risks with varying impacts and costs on the decision-maker, the tax system and the law. Decisions such as whether to flag a client's suspicious behaviour, whether to enact further due diligence, operational decision-making in a context of resource constraints, tax authorities making decisions to improve tax compliance, and policymakers deciding on new frameworks and guidance for MS to address tax crime. While this risk methodology will only play a part in all those decisions, it is designed in a way to render effective decision-making more possible in such an environment.

The risk assessment model will allow the user to identify risks, define priorities and self-assess practical steps and appropriate actions to mitigate the risk identified. The use of this risk assessment methodology is also contingent on context and can be used for reporting issues related to tax crime (e.g., by enablers), for training, and by policymakers and tax authorities to identify risks in and across their jurisdictions.

1.2 The risk assessment process

The purpose of this two-level risk assessment methodology can be summed up as follows:

1. To optimise decision-making for stakeholders in an environment of uncertainty (whether as part of their duties or as a training tool)

2. To identify policy frameworks and institutional, cultural and human factors critical to minimising tax crime risk.

It will achieve these purposes by providing a model with which to identify and alert the user to red flags indicating tax crimes (risks), but to also then identify other risks and vulnerabilities that may interfere in the successful detection, control, investigation and prosecution of such red flags. These vulnerabilities, as mentioned, are the human, cultural, legal and institutional factors discovered by PROTAX during work packages 1 – 6.

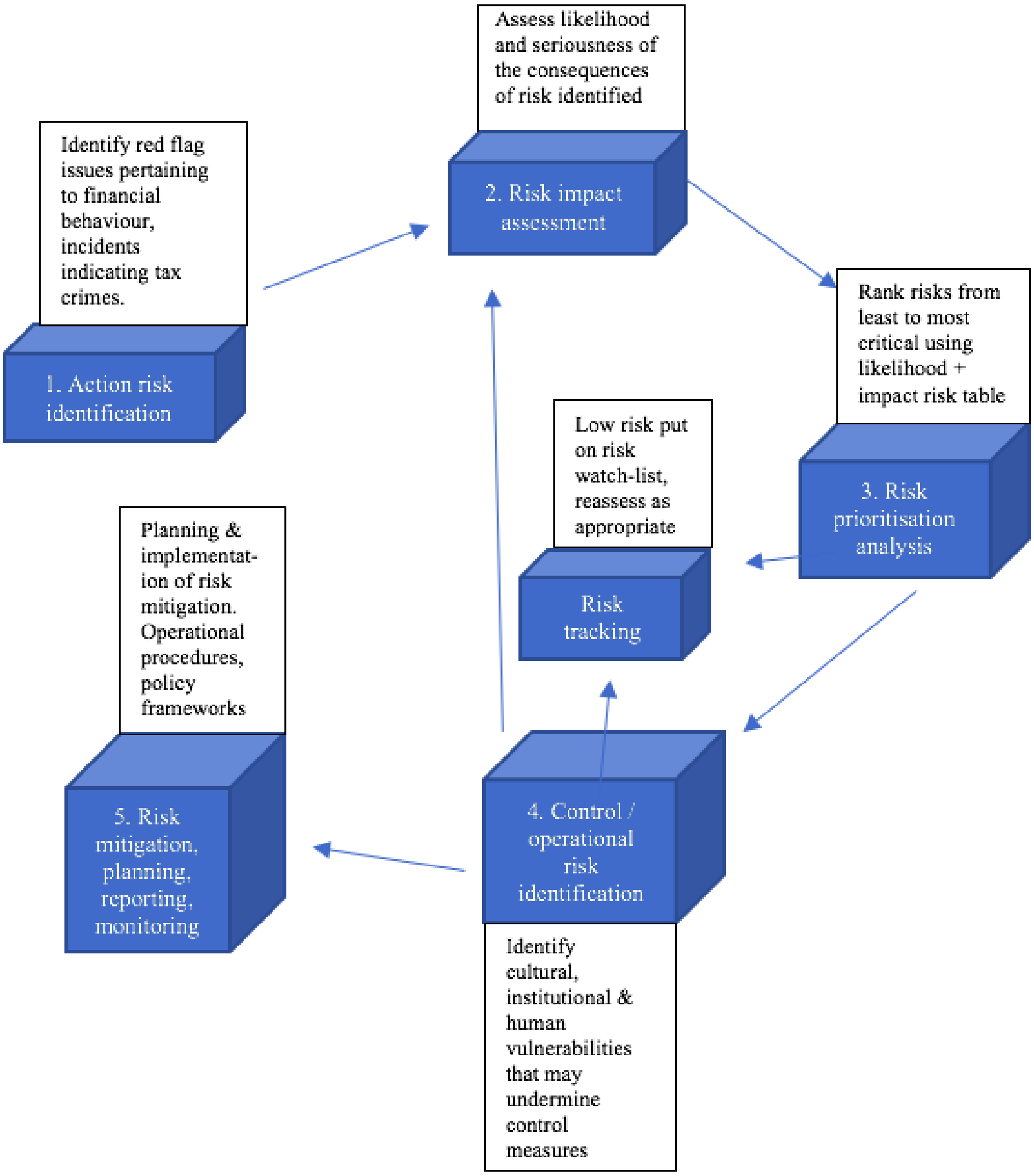
There are two interpretations of risk in PRORAM:

1. The first risk is that of a tax crime being committed. This relates to suspicious activity and incidents (red flags). These red flags are produced by answering the questions in Annex 3.
2. The second type of risks are the vulnerabilities that may produce a risk that these red flags cannot be resolved in an optimum way – these include the various legal, institutional and cultural factors identified in WPs 1 – 6.

This two-directional risk landscape (risks of a tax crime and risks to controlling those risks) drives the methodology developed in PRORAM.

Once a type of red flag behaviour is identified, an assessment model allows the user to rate the risk produced by the red flag by assessing its likelihood (or probability) and severity (impact or consequence). This prioritises decision-making. Next, the model will identify risks that may undermine the ability to control this risk (e.g., legal frameworks, differing tax crime thresholds, lack of information sharing, cultural, institutional and human factors). With this information, the user can choose to reassess the impact, choose to move to risk acceptance and monitoring or take risk mitigation measures by deciding on which actions to take (see chart 1 below and risk tables in Annex 2. Some of these risk mitigation measures will be developed in co-creation with expert stakeholders as part of WP8. It will also be up to the user to decide during their work or as part of a training exercise what risk mitigation measures are most appropriate, as these will be unique to different organisations and institutional settings. Risk mitigation measures will also interact with the recommendations provided in the other toolkits developed by PROTAX (D7.1, D7.2). The first toolkit addresses the legal and policy frameworks, and the second operational toolkit aims to transform information into intelligence for LEAs. The methodology by which the identification, assessment and prioritisation of risk is conducted, is detailed in section 4. The following chart conceptualises the risk assessment process.

Chart 1 – Conceptualising the risk assessment process


Identify red flag issues pertaining to financial behaviour, incidents indicating tax crimes.
1. Action risk identification
Assess likelihood and seriousness of the consequences of risk identified
2. Risk impact assessment
Rank risks from least to most critical using likelihood + impact risk table
3. Risk prioritisation analysis
Low risk put on risk watch-list, reassess as appropriate
Risk tracking
4. Control / operational risk identification
Identify cultural, institutional & human vulnerabilities that may undermine control measures
Planning & implementat-ion of risk mitigation. Operational procedures, policy frameworks
5. Risk mitigation, planning, reporting, monitoring

1. **Risk identification (red flags)** – *Identifying potential threats:* This is the role of the professional user [including banks, financial institutions, enablers and professionals with reporting duties]. However, as mentioned, we have created a set of questions that may indicate a tax crime (see Annex 3).
2. **Risk assessment** – This process assesses the *likelihood* that a certain behaviour under consideration indicates a tax crime, and *impact* assesses the seriousness of the potential consequences of that behaviour or incident or activity under consideration. The resulting score will denote the seriousness of the red flag.
3. **Risk prioritisation and analysis** – Risk prioritisation is ascertained in this stage by using both qualitative and quantitative measures produced in the risk assessment. As a result of this prioritisation, the user can move the risk to the monitoring stage or to risk mitigation.
4. **Control risk identification –** *Identifying vulnerabilities:* In this stage, the user should identify and evaluate any human, institutional and cultural factors that increase the risk that red flags cannot be controlled. PROTAX has populated some of this information in Annex 2 by drawing on WPs 1 – 6 and in conjunction with stakeholders and LEAs. If no particular risks are identified here, the risk can be moved to risk tracking and monitoring.

   Note: Step 4 has been placed after steps 1 to 3 in the process above to indicate that it is a separate analysis. However, step 4 (which are the risks identified in steps 1 – 3) is present at all stages, even if conducted separately. This will be expanded in the risk methodology section below.
5. **Risk mitigation (actions) –** This stage involves self-assessment by the professional using the risk methodology. PROTAX will include relevant findings from WP 1 – 6 to guide users.

It should be noted that while risk assessment can appear to be a sequential process it is in fact iterative, meaning that the desired result is achieved by repeated cycles of the process, producing increased understanding and improved treatment of risk.[10]

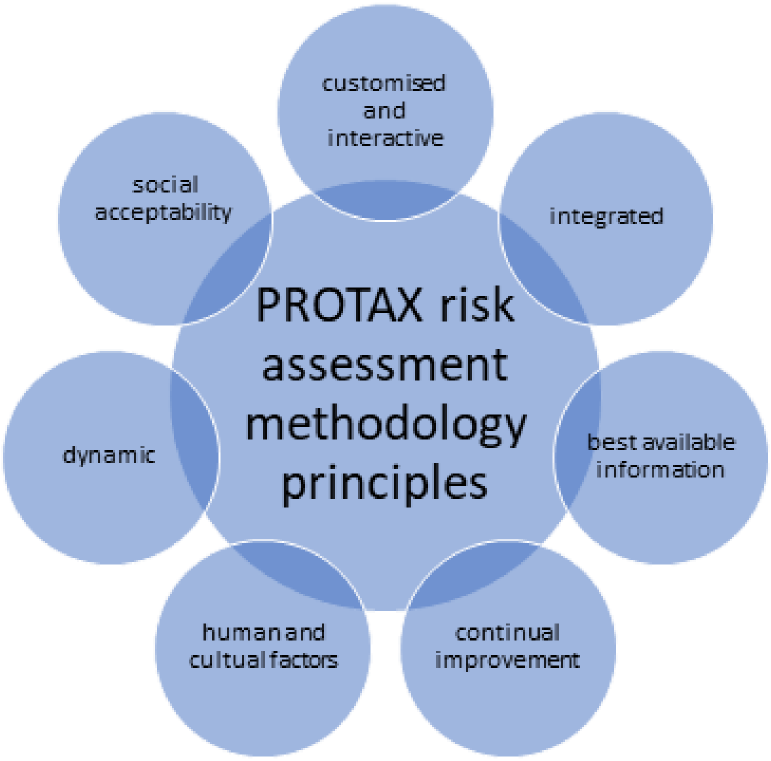
1.3 Risk assessment principles

To be effective in the fast-changing tax crime environment, the PROTAX risk assessment methodology (PRORAM) will be driven by the following principles:

Chart 2[11]

[10] ISO international standards, 'Risk management guidelines', 2nd edition, ISO 31000 2018(E), 2018, [p9].

[11] Chart adapted from: ISO international standards, 'Risk management guidelines', 2nd edition, ISO 31000, 2018.


customised and interactive
social acceptability
integrated
PROTAX risk assessment methodology principles
dynamic
best available information
human and cultual factors
continual improvement

a) Integrated – PRORAM will be integrated with organisational operations of enabler organisations, FIUs, tax authorities and policy makers as well as with the other PROTAX toolkits being developed that optimise policymaking and the investigative efficiency of LEAs.

b) Customised and interactive – PRORAM can be customised to organisational needs and institutional objectives of the users, enabler organisations, tax authorities and policymakers. PRORAM is interactive, meaning stakeholders across MS will be able to input data, information and assessments to an interactive platform. This will continually improve effectiveness and build the informational capacity of PRORAM.

c) Best available information – Drawn from PROTAX WPs 1 – 6, our original findings of the human, institutional and cultural factors involved in tax crime will provide inputs to PRORAM. This is augmented by PRORAM being interactive and customised, drawing on the best available information from expert stakeholders.

d) Continual improvement – Continual improvement of information, accuracy and reflective assessment is key to co-creating and testing PRORAM with stakeholders, and the use of the PRORAM within organisational settings and training. This will be the role of end users.

e) Human and cultural factors – PRORAM assesses the uncertainties and risks inherent in investigating and prosecuting tax crime produced by human, institutional and cultural factors. This will be drawn from the PROTAX work already done in WPs 1 – 6.

f) Dynamic – New risks can emerge or current risks can dissipate due to organisational change, the innovation of tax criminals or policy frameworks. PRORAM will be attuned to this reality and remains able to respond to evolving tax crime environments. The best available and most current information is also key to maintaining this dynamism. PRORAM will also be dynamic insofar as it mirrors the inter-jurisdictional nature of tax crimes by accounting for the intersecting risk pressures produced by cross border tax crime and investigation.

g) Social acceptability – Social acceptability requires that the development and use of PRORAM avoids unnecessary targeting of ordinary EU citizens. This is achieved by ongoing privacy and ethical impact assessments at key decision-making junctures.

Before going into more detail about the Failure Modes Effects Analysis (FMEA), which is the actual methodology used to evaluate and treat risk, the next section will detail the justifications behind the two-level approach, first with a discussion of the KYC type level, which identifies red flags (potential threats) and the EU-wide risk assessment framework (potential vulnerabilities).

2. Risk assessment level 1 and level 2

2.1 KYC risk assessment– identifying red flags [Level 1]

The first level of the tax crime methodology is a KYC type risk assessment for enablers that is specific to tax crime. KYC is a common practice across the financial sector and refer to the process by which banks, financial institutions, non-financial institutions and professionals with reporting duties fulfil their various jurisdictional and legal obligations to verify that a customer is who they say they are, the ultimate beneficial owner of their financial assets is clear, transactions are explainable and their financial behaviour is legitimate.

Enablers (or obliged entities) are required by the 4th and 5th AMLD (Anti-money laundering directives)[12] to conduct a business risk assessment directed at money laundering (ML) risks and mitigating measures tailored to their business and operations. Such obliged entities are also required to conduct a customer risk assessment (CRA) before ‘on boarding’ a customer to assess client risk and to ascertain whether the outcome of that assessment falls within their risk appetite. Based on the outcome of that risk assessment (and identification of where the risk lies), obliged entities are required to vary their customer due diligence (CDD) practices accordingly, on a risk-based approach.

There are a number of existing anti-money laundering (AML) KYC models of this type in existence and we do not wish to replicate this type of risk assessment. The PROTAX risk assessment will alert enablers to potential red flags denoting a suspicious transaction or financial arrangement in the first instance, but then try to embed that risk within the vulnerabilities and risks of the wider tax crime eco-system of the EU. Typically, suspicious ‘red flags’ often only identify ‘illicit financial flows’ (IFF) of some kind, and as such, these cannot usefully predict what predicate offence lies behind that illicit flow. Proceeds

[12] European Parliament and the Council, Directive (EU) 2018/843, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, Brussels, 30.5.2018 https://eur-lex.europa.eu/eli/dir/2018/843/oj .

of tax crime are often laundered and may be being used for other criminal enterprises, so IFF are inextricably related to tax crimes and tax fraud is suspected to be behind 39% of STRs).[13]. What level one of PRORAM attempts to do is add value for the user to identify IFFs that are also potentially linked to the predicate offence of tax crime. This has been done by drawing input variables from the extensive work conducted in PROTAX WP 1 – 6, and exploiting the knowledge of the PROTAX consortium, partners and stakeholders involved in tax crime, such as LEAs and FIUs. To achieve this PRORAM includes questions (see annex 3) to identify customers and behaviour that may specifically link to the predicate offence of tax crime.

It should be noted, however, that LEA partners have already informed PROTAX that due to the nature of the risk, many red flags used internally by LEAs are classified. This is to prevent tax criminals innovating and altering behaviour once they know which behaviours are considered suspicious. As such, the professional's judgment and input variables from end users will be relied on in this step, in addition to the questions already generated by PROTAX in conjunction with LEA partners. This also justifies the need for a thorough review process through which emerging risks (and changing behaviours) can be assessed and treated, and a dynamic and interactive approach to inputting risk data by users, which will be incorporated into the final interactive end product toolkit.

To ensure that the PROTAX risk assessment model has sufficient data to be usefully predictive and valuable, WP8 demonstrations will be used to identify gaps in the data and typology of risks, develop strategies to fill those gaps and isolate problems and resolve them. For this level of the risk assessment methodology to add value, therefore, we must engage closely with LEAs for valuable input variables indicating red flags, develop reporting best practices and make the risk assessment methodology interactive and open to constant review of red flag behaviours, and add pertinent questions for enablers and professionals on an ongoing basis as and when necessary.

This level of the risk assessment methodology can be adopted and used by enablers in their professional role or can be used as a best practice training tool for enablers and other professionals with reporting duties. More details of how it can be used is found in **3. Use cases** section and in **4.2. How it works: Process guidance for FMEA** section. The idea is not to replicate the extensive KYC and CDD models already out there, which comprehensively address legal risks to enablers, but to draw enablers into thinking about the tax crime risk landscape more broadly in their professional role, taking in vulnerabilities, uncertainties and institutional differences, and thinking about this in terms of risks. The knowledge generated by this level of PRORAM in conjunction with level two is also designed to influence policy makers who interact with enabler organisations. One of the key dilemmas PROTAX has identified is that enabler organisations who commit tax crime, are also 'at the table' with EU policy makers deciding on policies to prevent tax crime. Inserting this risk assessment methodology into that

[13] Europol, Financial Intelligence Group, 'From suspicion to action - converting financial intelligence into greater operational impact', Brussels, 05.09.2017. https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact .

policy making environment (see **3. Use cases** section) can have impact on the behaviour of those enabler organisations.

The set of questions have been developed in conjunction with LEA partners from the PROTAX consortium and research of common questions found within industry KYCs. These questions aim to highlight behaviours that should be considered as a red flag risk that may indicate the predicate offence of tax crime. The self-assessment questions (Annex 3) are, however, intended as a guide. The most useful diagnosis will be achieved when used by professionals with more intimate knowledge of tax crime in their work. This is because factors are unique to each situation and enablers must get to know their client and use their judgment in order to properly assess their risk. The important factor for enablers when looking at a transaction or financial arrangement is to question the logic of the transaction or behaviour they are considering; understanding the logic of the transaction or otherwise is dependent on knowing the customer's normal financial dealings. However, the questions in annex 3 act as a basis for assessing suspicious transactions and behaviour, and the FMEA risk assessment encourages enablers to assess whether they can control those risks successfully when thinking about the broader tax crime law enforcement eco-system. This will feed into level two, which looks at risks to controlling the risks produced by suspicious transactions.

2.2 EU-wide systematic risk assessment framework – identifying vulnerabilities (Level 2)

Most risk assessment methodologies related to tax crime are focused on illicit financial flows on a national or geographic basis. The EUs eight building blocks for assessing risk of money laundering similarly focusses on assessing the risk presented by external 'third countries'.[14] The PROTAX risk assessment approach adopts a similar framework, but the aim is to apply it internally to the workings of the tax crime law enforcement ecology of the EU. This will uncover vulnerabilities that enhance the risks of tax crime for EU members states qua EU member states. In line with the OECD[15] and World Bank[16] risk assessment methodologies, PRORAM provides a framework for self-assessment for EU policy makers, tax authorities and individual EU member states related to the risk priorities identified in PROTAX WPs 1 – 6. These areas, as mentioned, are:

Scope and definitions of tax crimes
Threshold of tax crimes
Sanctions for tax crimes
Legal liability for tax crimes

[14] European Commission, Methodology for identifying high-risk third countries under Directive (EU) 2015/849. Commission staff working document, SWD (2020), Brussels, 7.5.2020.

[15] The OECD 'Maturity Model' is yet to be published. However, discussions on its approach have taken place with a senior tax crime advisor from the OECD, who is also on the PROTAX stakeholder board. The Maturity Model is a way for countries to assess the stage at which their tax crime law enforcement environment – legally, institutionally and operationally – is 'mature' by international standards.

[16] World Bank, 'Risk Assessment Support for Money Laundering/Terrorist Financing', 2016 https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support

International cooperation on criminal matters
Information sharing
Whistle-blower treatment
Obligations to report suspicious financial behaviour
Obligations to maintain secrecy of client's financial transactions (transparency versus secrecy)
Resource constraints

This enables the user of the risk assessment to identify and prioritise areas of high risk, and identify areas in which legal, policy, cultural or organisational changes could lower the risks of tax crimes and improve the EU investigation and prosecution environment.

The purpose of this risk assessment methodology is to build knowledge of these vulnerabilities within the system of tax crime compliance, investigation and prosecution of tax crime, and encourage harmonisation to 'design out' the risks produced by them. The method by which this is done is set out in section **4. PROTAX Risk Assessment Methodology (PRORAM): Failure Modes Effects Analysis (FMEA).** Specific uses envisaged for the risk assessment framework to generate impact is for the European Commission to use it to encourage member states to address certain vulnerabilities, for tax authorities of member states to adopt the risk assessment methodology as an internal document and for various tax crime law enforcement stakeholders to work through the risks together at workshops and training events (see, ***Use Cases*** section for more details). Using it in this way can encourage harmonisation in the areas identified as creating risks for EU members states. This aligns with the approach that countries using the World Bank's risk assessment methodology[17] are being encouraged to adopt and the OECDs 'Maturity Model'[18]. It is important to identify the right policy makers, authorities and contacts across the EU and in the EC to adopt this approach or be influenced by it.

Taken together this two-level approach to tax crime risk also addresses the EU framework on money laundering provided by the fourth 'Anti-Money-Laundering Directive', which identifies money laundering risks at three levels: at supranational level, at MS level and at the level of the obliged entities as part of their CDD responsibilities.[19] The use cases we outline match these priorities.

3. Use Cases

A key discovery during PROTAX has been the intersecting responsibilities and roles played by different stakeholders within tax crime investigation and enforcement. From policy makers at both and EU and MS level, to FIUs, tax authorities, LEAs and enabler organisations. Breaking silos and sharing information in this context is key, and this keenly applies to identifying and treating risk. In this context, PRORAM can be used in a number of different scenarios to increase value for tax crime law

[17] *Ibid.*

[18] The OECD 'Maturity Model' [see, footnote 14 above].

[19] European Parliament and the Council, On the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Directive (EU) 2015/849, Brussels, 20.5.2015.

enforcement stakeholders. The following case studies are examples of how PROTAX envisages the risk assessment methodology to be used to have impact on the harmonisation of laws, policies and EU best practice as a way to reduce the risks of tax crime for the EU.

3.1. Use case one: Training tool for enablers and other professionals with reporting duties

Enablers and enabler organisations (such as accountancy firms, banks, real estate agents and financial services providers) have a central role in both tax crime and the tax crime law enforcement eco-system. On the one hand they are often duty bound to conduct aggressive tax planning on behalf of their clients, on the other hand they have legally obligated reporting duties, such as those found in the AML 4th and 5th directive.[20] Moreover, while they are subject to EU policy and law-making on tax matters, PROTAX discovered that they are also often 'at the table' when such policy is being decided upon. The contradictory roles that enablers play is a particular problem for the tax crime law enforcement environment and was investigated in detail in WP1 and WP6. Engaging enablers and professionals with reporting duties with the PROTAX risk assessment methodology is a way to integrate wider issues of tax crime law enforcement into their professional practices, beyond the limits of their client relationships and legal obligations. This use case entails holding a series of EU-wide one day workshops and training events for enabler organisations, and to encourage responsible enabler organisations already engaged in EU policy making to trial the PROTAX risk assessment methodology within their companies. This can encourage such companies to take a more holistic view of risks within the tax crime law enforcement environment by training them to understand that there are risks inherent to their professional role that go beyond legal obligations and client interests. This 'training tool' style use case is in line with the PROTAX grant agreement.

3.2. Use case two: Member State risk assessment workshops

PROTAX has investigated discrepancies and vulnerabilities on an inter-jurisdictional basis. However, it is also true that within MS vulnerabilities and uncertainties in the tax crime law enforcement environment carry risks to the successful investigation and prosecution of tax crimes. For example, PROTAX discovered in the focus groups (WP2) that institutional and departmental information sharing was an issue in many member states. The sub-optimum quality of the relationships between different administrative functions within MS, due to silos, was also found to carry risks. Additionally, some jurisdictions are more attractive to tax criminals due to factors such as higher thresholds for tax crimes or resource constraints within tax crime law enforcement institutions of a MS. In this environment, information sharing, prioritising risks and coordinating action within a MS in order to reduce risk can be challenging for LEAs, tax authorities and policymakers. Knowledge building and knowledge sharing of these risk issues can be produced by bringing together stakeholders from within the tax crime law enforcement environment of a MS to work through the PROTAX risk assessment methodology

[20] European Parliament and the Council , On the prevention of the use of the financial system for the purposes of money laundering or terrorist financing Directive (EU) 2018/843, amending Directive (EU) 2015/849 and amending Directives 2009/138/EC and 2013/36/EU, Brussels, 30.5.2018 https://eur-lex.europa.eu/eli/dir/2018/843/oj .

together. By identifying risks specific to that MS, such as particular resource constraints or information sharing deficiencies, these risks, and therefore areas for action to improve tax crime law enforcement, can be identified and prioritised on an inter-institutional level. This risk information can also then be shared with partner institutions (as appropriate) from other MS to improve harmonisation and share knowledge across and between MS. Because risk assessment and risk management are iterative, PROTAX recommends at least annual risk assessment workshops involving relevant stakeholders within each MS. At these workshops, stakeholders can identify and prioritise risks, share knowledge and decide collectively upon control measures and actions to improve the functioning of the tax crime law enforcement environment on an ongoing basis.

3.3. Use case three: EU-level risk assessment workshops

PROTAX has conducted significant comparative work on the tax crime law enforcement environment of the EU, discovering many uncertainties and vulnerabilities that can be usefully modelled as risk. These include contrasting typologies of tax crime across jurisdictions and varying (cultural and legal) treatment of whistle-blowers and tax crime across Member States. One of the key challenges PROTAX addresses is to contribute to harmonising prosecution modes and tax law across the EU, along with improving information sharing and addressing human factors. This use case demonstrates how this can be done. Stakeholders from across the EU, in the first instance through networks already developed by PROTAX, should be brought together to hold a series of workshops in order to work through PRORAM. In a similar fashion to the workshops on a MS level detailed in **use case 2**, stakeholders can work through the risk assessment – from the risk of a threat identified in a suspicious transaction, through to successful prosecution. In doing so, stakeholders can identify policy improvements, best practices and alignment of key areas, and where possible design out vulnerabilities. While this will not instantly produce the answers necessary to harmonise law and best practices across the EU, collectively highlighting priorities by using PRORAM can contribute in a valuable way towards that.

3.4. Use case four: Policymakers adopting PRORAM as an internal best practice document

The importance of considering not only the black letter of the law (law in books) but also law in action is a recurring theme in PROTAX analysis and recommendations. Likewise, harmonisation of tax crime law enforcement is not only achieved through setting specific policy or regulatory limits, but also through harmonising best practices and information exchange. In this use case, we encourage EU policymakers to adopt PRORAM as an internal best practice document. This will contribute to harmonisation on two levels:

i) Within EU policymaking itself, as policymakers use the risk assessment to identify and address key vulnerabilities across the EU in the tax crime eco-system.

ii) Through best practice recommendations communicated to stakeholders by EU policymakers.

4. PROTAX risk assessment methodology (PRORAM): Failure Modes Effects Analysis (FMEA)

4.1 FMEA explanation

This section describes the methodology adopted and developed for PRORAM, followed by examples of how it works. Due to both the national and international nature of tax crime, its cross-border flows and connections, its jurisdictional interoperability and the extent to which illicit financial flows are integral to tax crime and its profits, PROTAX proposes a risk methodology that adapts methodologies used commonly in risk assessments of systems and processes, often found in sectors like global supply chains or product development – failure modes effects analysis (FMEA)[21]. This is because the purpose of FMEA is to take action to eliminate or reduce failures, by 'designing' identified failures out of the system. Designing out failures in the tax crime law enforcement eco-system of the EU entails harmonisation across a spectrum of areas – institutional, legal, cultural – and it is to this purpose that PRORAM and the PROTAX project is directed. Using this risk methodology will allow stakeholders to identify areas in which action can be taken to optimise the investigation of specific tax crimes or mitigate against risks that undermine the ability to prevent or reduce tax crimes in and across EU jurisdictions.

'Failure modes' in FMEA means the ways in which something *might* fail. Failures are errors or defects that, in this context, potentially impact upon the tax system. Failures can be potential or actual. In other words, 'red flag' behaviour *may* indicate a tax crime, and this requires further due diligence to discover if this is the case. The fact that a particular behaviour may indicate tax crime is sufficient to be considered a risk and addressed as such in this model. 'Effects analysis' refers to studying the potential consequences of those failures.[22]

FMEA focusses on the importance of 'control' (C), which are the measures that exist to detect, prevent or mitigate the risk identified as a potential failure mode (F). A failure mode can be considered as the manner in which the operation fails to meet the requirements. Suppose that one failure mode is identified, for example, the inability to identify a corporate account suspected of a tax crime. One step of FMEA is to investigate the 'causes' and 'effects' related to this failure mode. So, in this case, this failure mode may have been caused by that jurisdiction's secrecy laws. The 'effects' of that could be that one node in an international VAT fraud cannot be investigated. Notably, causes and effects are identified by focusing on one failure mode at a time, and the causal chains of the failures are of particular concern in FMEA (unlike, for example, Fault Tree Analysis).[23] This model has been

[21] ISO, Design FMEA, 12132:2017(en), 2017, https://www.iso.org/obp/ui/#iso:std:iso:12132:ed-2:v1:en

[22] Carlson, C.S., Understanding and Applying the Fundamentals of FMEAs, *2016 Reliability and Maintainability Symposium*, 2016. https://www.weibull.com/pubs/2016_RAMS_fundamentals_of_fmeas.pdf .

[23] Li, S., Zeng, W., Risk analysis for the supplier selection problem using failure modes and effects analysis (FMEA). *Journal of Intelligent Manufacturing*, Vol. 27**,** 2016, pp. 1309–1321. https://doi.org/10.1007/s10845-014-0953-0 .

chosen because it is useful for identifying and analysing vulnerabilities and the connections across the complex tax crime environment that are acting as causes, uncertainties and vulnerabilities, contributing to the proliferation of tax crimes. These causes will be modelled and assessed in level two of the risk assessment methodology.

This risk assessment methodology aims to uncover tax crime risks within the EU and uncertainties and vulnerabilities that increase the risk of a tax crime being committed as well as increase the risk of a tax crime not being detected, prevented or prosecuted. Many tax crimes span borders, and as such investigations need to do so too. The legal, institutional and cultural differences between MS in which a tax crime is committed are therefore factors in the risks of a tax crime being committed, and the risks to successfully detect and prosecute it. Such discrepancies and vulnerabilities are modelled as risk in Annex 2, details of which have been produced by the work conducted in WPs 1 – 6 and in co-creation with the PROTAX consortium and stakeholders.

The basic causal relationship of a failure mode can be conceptualised as:

"cause(s) → failure mode → effect(s)"[24]

For example, secrecy laws of a particular jurisdiction (cause) prevent financial transparency of a suspect corporate account (failure mode) which in turn prevents full investigation and prosecution of an international VAT fraud (effect). The effects can be qualitatively assessed by experts to understand their seriousness, and which risk mitigation measures or actions are appropriate. This allows a holistic risk-based approach to be taken for complex tax crimes, and for different stakeholders to come together to 'design' out these risks.

To assess the risks that may produce a failure mode, FMEA analyses risks in three dimensions: likelihood, impact and control. While the concepts of likelihood and impact are typical in risk management, the control concept of FMEA is concerned with the techniques to avoid or mitigate the risks. This is the second level of the PROTAX risk assessment methodology. Risks to control factors for PRORAM are, as mentioned, factors such as legal gaps in prosecution of certain types of tax crime, discrepancies in typologies of tax crime and tax crime thresholds between jurisdictions.

To evaluate each of these three dimensions, a 10-point scale is used in FMEA. The higher the score is, the worse the case is for each dimension being evaluated. In other words, scoring a 10 for 'control' means that control has completely failed, a 10 for likelihood means whatever is being evaluated is inevitable, and so on. The risk priority number (RPN) is obtained by adding the score associated with control (C) and likelihood + impact (severity (S)) in level one, and by adding the score associated with risk evaluation (E), control (C) and likelihood + impact (severity (S)) in level two. Using FMEA in analysis of tax crime and its investigation ties the risk of an actual tax crime and its potential severity with the risk that is present in not being able to control that risk. Severity is assessed by the user evaluating the likelihood the tax crime will happen plus the impact on the tax system if it does, interpreted as the

[24] *Ibid.*

amount of money involved in the tax crime or the frequency with which that tax crime occurs. The user can use this methodology for addressing questions such as: is this risk severe? Can it be controlled or detected? What measures can I take to improve control measures?

This control aspect is vital for assessing the legal, cultural and institutional factors identified in PROTAX WPs 1 – 6 that can potentially undermine investigation and prosecution of those tax crimes. It guides users towards identifying risks inherent to certain policy environments, professional decisions and investigation scenarios, and indicates where operational or policy improvements are required in order to mitigate risks to the financial and tax system. This is not, however, an LEA enforcement toolkit. The D7.2 toolkit addresses this. However, by identifying risks in the enforcement environment using this risk methodology, policymakers and tax authorities (and LEAs) can make considered judgements about operational, institutional and policy changes that could aid operational effectiveness. The value of PRORAM is that it not only identifies tax crime risks and failure modes, but will allow the end user to analyse the types of uncertainties and vulnerabilities produced by such factors at an EU level that may produce risks that undermine the ability to optimise the *control* of red flag risks.

Some of the same indicators that may alert a red flag risk issue in a financial transaction can also impact the extent to which LEAs, tax authorities or enablers can operationally respond to that risk (the control risk). For example, a hostile environment for whistle-blowers may increase the risk rating that a certain enabler company is likely to be engaged in a tax crime (if coupled with another risk indicator relating to suspect financial behaviour). This simultaneously makes it hard for LEAs to get information about such risks. So, the same risk factor is preventing the optimum operational response to that risk.

Similar double risks (of failure and control) pertain to factors such as a jurisdiction's secrecy laws, lack of inter-agency information sharing, resource constraints and cross-border financial flows. Details of these have been generated in co-creation with stakeholders, will have further input during WP8 demonstrations and will be up to end users with professional expertise using the risk assessment to populate and assess.

4.2 How it works: Process guidance for FMEA

The following table is a step-by-step guide to this FMEA risk assessment.[25] More detailed guidance is provided in Annex 2.

1. Identify the functions of your scope. Ask: what is the purpose of this system, design, process or service? Are the functions in this context lawful and proper financial transactions?

[25] Adapted from: Stamatis, D, H., *Risk Management Using Failure Modes And Effects Analysis (FMEA),* ASQ, Wisconsin, 2019, and, Nancy R. Tague, *The Quality Toolbox*, Second Edition (E-Book), Quality Press, 2005

2. For each function, identify all the ways failure could happen. In the case of tax crime, the function can be broadly defined, as above. These are potential failure modes. If necessary, go back and rewrite the function with more detail to be sure the failure modes show a loss of that function, e.g., tax crime, failure of compliance, VAT fraud, suspicious transaction.

3. For each failure mode, identify all the consequences on the financial system, related internal systems, company, customers and tax law regulations. These are the potential effects of failure. Ask: What happens when this failure occurs? What is the effect (size) of this suspect transaction? How much money? How serious?

4. Once you have reflected on the effects qualitatively in this way, determine how serious each effect is. This is the severity rating, or S. This is obtained by using the risk table in Annex 1a (calculation likelihood + impact). Severity is rated on a scale from 1 to 10, where 1 is insignificant and 10 is catastrophic. If a failure mode has more than one effect, write on the FMEA table only the highest severity rating for that failure mode.

5. Identify and assess current process controls. These are tests, procedures or mechanisms that you now have in place to prevent failures from reaching the tax system. These controls might prevent the cause from happening, reduce the likelihood that it will happen or detect failure *after* the cause has already happened but *before* the tax system is affected. (e.g., enhanced CDD on customer, information sharing with FIUs, LEAs). This is scored by using the control evaluation table in Annex 1c .

6. Calculate the risk priority number, or RPN. In the level one the RPN score is S (likelihood + impact) + C. These numbers provide guidance for ranking potential failures in the order they should be addressed.

7. Identify recommended actions. These actions may be process changes, information gathering, reporting or additional controls to improve detection. The aim of the actions is to lower the RPN.

8. At this point, repeat the FMEA for the control measures (level two). This can be done for training purposes and knowledge building involving tax authorities, policymakers and LEAs. Failure modes in the control measures could include what is most likely to prevent detection or produce sub-optimal investigation or prosecution of tax crime. This includes things like lack of cooperation, lack of information sharing, ineffective tax crime sanctions regime, corporate secrecy, etc.

9. Once the level two RPN is calculated (which is E + S + C), move onto actions to be completed to address it and lower the RPN. How, by when, who? – e.g. policy change, breaking silos, cultural shift, information sharing etc.

Both levels can be used by policymakers and tax authorities. By identifying a red flag through the risk assessment questions (Annex 3) and following the process through to assessing how the different vulnerabilities present a risk to controlling that red flag, the user can identify where risks are in the chain from ‘red flag identified’ through to ‘successful prosecution’. This process could be conducted in collaborative training exercises involving different tax crime law stakeholders from across the EU or within MS (see **use cases** section).

The tables in Annex 2 set out the failure modes, control failures and effects identified in the PROTAX project WPs 1 – 6. Annex 3 sets out questions for enablers to assess failure modes, produced in co-creation with LEA and FIU stakeholders in the PROTAX consortium. This data ought to be used in conjunction with this risk methodology. However, diagnosis of risk will be optimised when professionals and other end users input their own variables and data on an ongoing basis. The failure modes discovered by PROTAX should, however, influence this.

4.3 How it works: FMEA risk assessment methodology examples

This section sets out working examples of PRORAM. The two-level FMEA approach to risk is detailed below. This assesses risks pertaining to tax crimes, in level one, and risks to controlling those risks produced in the legal, institutional and operational environment of the EU, in level two. Below is a worked-out but simplified example of how the risk assessment methodology could be used in practice. The completed columns are merely examples to demonstrate the process.

In the example below, the hypothetical user has discovered a suspicious transaction by using the red flag questions in Annex 3, the ‘effects’ of this is conceived by the size of the suspicious transaction (€10,000). The user has calculated the S score by assessing the likelihood that this suspicious transaction is a financial crime of some kind and the impact of the crime it indicates. Impact is assessed by the user reflecting on the ‘effects’ (i.e. €10,000). The user has then assessed control measures, discovering that they cannot identify to whom the transaction benefited, scoring that accordingly. Finally, the user has filled in actions necessary to lower the risk, which is to get information about the unknown beneficiary. The user has then moved onto level two to assess the risks to the control measures present in level one. In this instance, why information about an unknown individual cannot be ascertained.

Table 1 - Level 1
This table assesses the threats to the tax / financial system. A ‘suspicious transaction’ failure mode is established by answering the questions in Annex 3. The scoring is purely an example (see Annexes for how to score E, S and C).

Failure mode (Use Annex 3 questions)	**Effects**	**Severity – (S) likelihood + impact (Use Annex 1a)**	**Control**	**Risk priority number**	**Actions recommended**
Suspicious transaction	€10,000	5	9	14	Seek information

			Unknown individual / beneficiary in different MS jurisdiction		about unknown beneficiary

Table 2 - Level 2

This table assesses the vulnerabilities that could potentially undermine the control factors in level 1 above. The failure mode here in level 2 is assessed on the basis of vulnerabilities in the tax crime law enforcement eco-system that may undermine control of the suspicious behaviour. The extra column here, 'evaluation of failure mode (E)', is to assess the failure of the control measures in table one, which in this example is 'lack of information sharing'. The scoring is purely an example based on a hypothetical user. It is important to re-iterate the potential uses that PROTAX envisages for PRORAM here, which is for multiple stakeholders to work through this together to understand *how* and *why* certain failure modes cannot be sufficiently controlled. In this example 'information sharing' is the key factor, but in other examples it will be other factors. Annex 2 has a series of these risk tables covering a range of failure modes and guidance to score them accurately.

Failure mode	**Evaluation of failure mode (E) (Use annex 2 tables)**	**Effects**	**Severity (S) - likelihood + impact (Use table in annex 1b)**	**Control**	**Risk priority number**	**Actions recommended**
Lack of information sharing	7	Unable to control suspicious transaction	8	7 No information	22	Engage FIU.net

This is the basic process. More detailed evaluation schemes for risks to 'control' and the evaluation schemes for 'failure modes' are in the tables in Annex 2.

Action risks to C in table 1 and 2 have been broadly and generally conceived for simplicity. It may be that in many instances there is no relationship between the control factors in level 1 and the risks to control produced in level 2. This process helps to discover those links as and when they arise. As the use cases show, multi-stakeholder engagement with the risk methodology can help discover these links if and when they arise, from red flag threat through to successful prosecution.

Specific C risk factors could include information sharing (undermined by the cross-border nature of tax crime), tracing of accounts (undermined by jurisdictional secrecy), insider information / evidence (undermined by legal, cultural and / or corporate hostility to whistle-blowers). C information will be co-created by experts and are up to the end user to input. Many of the risks to C, however, are provided by the PROTAX project work packages 1 – 6 and are in the tables in Annex 2.

Taken together, this can produce a clear line of sight in operational, policy and institutional weaknesses. While scoring it quantitively in this way is useful, the key value of the methodology is to operate as a practical guide to expert decision-making. It is also up to the experts to score it quantitively based upon their judgment, giving them a way to rank risk priorities based on their own assessments.

The key risk factor identified in this example is the 'unknown individual / beneficiary'. This denotes the inability to control the failure mode identified, which is a suspicious transaction. The aim of PRORAM is to understand, calculate and then provide space to mitigate any risks that are undermining the ability to control the failure mode identified in this way, e.g., identify the individual.

So, in this case, the risks that undermine the ability to identify the 'unknown individual' (or source of the transaction) would be identified and assessed. There can be multiple risks to the control measures, ranging from different jurisdictional thresholds on tax crime, to information sharing, corporate secrecy and so on. Evaluation of the risks to C will be the role of the professional or expert engaging with the risk methodology in a given context. However, PROTAX has generated a lot of information regarding institutional, legal and cultural risks to successfully controlling a red flag risk.

Another example from the Annexes of an 'evaluation scheme' for assessing risks to control measures is the below table. PROTAX has identified the following key issues with whistle-blowers: corporate attitudes, legal protections and cultural attitudes. Below is an example of how the treatment of whistle-blowers in a certain context, understood as risk, can be evaluated and scored to assess the extent to which it may undermine the ability to control (C) a failure mode in a given instance.

Table 3 Evaluation scheme for assessing risks to C

Whistle-blower risk assessment score

Rank	***Corporate attitudes to whistle-blowers***	***Legal protection of whistle-blowers***	***MS cultural attitudes to whistle-blowers***	***Risk score***
10	A demonstrably hostile corporate environment for whistle-blowers	Prosecution of whistle-blowers highly likely	Hostile ("snitch", "grass" etc)	

8-9	A difficult corporate environment for whistle-blowers	Prosecution of whistle-blowers quite likely	Culturally hostile but acceptable in certain circumstances	
6-7	No corporate support	Prosecution of whistle-blowers possible	Ambiguous but generally negative	
4-5	Some minimal corporate support	Minimal legal protections for whistle-blowers	Ambiguous but generally positive	
2-3	Corporate support but without specific and / or robust corporate whistle-blower policy	legal protections for whistle-blowers	Generally positive attitudes to whistle-blowers	
1	Corporate support embedded within robust company policy	Robust legal protections for whistle-blowers	Positive attitudes to whistle-blowers (“public champions”, “heroes” etc)	
Whistle-blower risk score	7	2	4	4.3

This requires stakeholder input and continual reflective assessment. Other evaluation schemes for C are set out in Annex 2. Below is the qualitative assessment of the evaluation of risks involving whistle-blowers, based on the work already conducted in the PROTAX project. Similar qualitative judgements can be applied by experts and users when they reflect on other risk factors pertaining to C in conjunction with other stakeholders in training events and workshops. Reflecting qualitatively in this way, whether in writing or through discussion, can then influence the score assigned in each instance.

Corporate attitudes to whistle-blowers – Some corporate environments encourage honesty and the reporting of wrongdoing, giving employees official avenues through which to share concerns. This generates an encouraging culture for whistle-blowing. Others, however, make the life of a whistle-blower untenable within the corporation, due to the behaviour of managers and/or colleagues. Such corporate consequences for the employee who blows the whistle sometimes extends across the industry, meaning whistle-blowers may struggle to secure gainful employment anywhere after blowing the whistle. This can be the case even if the law protects them. Corporate attitudes, therefore, strongly influence the extent to which employees and staff of enabler companies are prepared to either report or hide wrongdoing, and produces a risk score for that company, based on the likelihood that wrongdoing will either be reported or hidden.

Legal protection of whistle-blowers – Even though EU-wide whistle-blower guidelines exist, laws vary across MS, and because both tax crime and many enabler companies are transnational, the legal protection of MS is important to consider as a motivating factor for hiding wrongdoing by employees. It is also the case that even if corporations have a good attitude towards whistle-blowers, some of their operations may be based in a country where whistle-blowing is illegal or poorly protected.

MS cultural attitudes to whistle-blowers – This risk is based on the differing cultural attitudes found across MS. It produces a risk because even if the corporate environment is conducive to whistle-blowing and whistle-blowers are legally protected, the normative cultural force of not wanting to be considered a "snitch" or a "grass", as whistle-blowers are linguistically defined in some MS, produces a risk of wrong-doing being under reported.

Whistle-blower risk score – The mean average of all three is calculated to denote a risk score for an enabler company with regards to a specific situation. Considerations in calculating the risk score are designed to take into account the transnational nature of tax crime environment. For example, if an employee from Estonia worked for a British bank operating in Switzerland, then the intersecting pressures on that employee from all of those factors and entities need accounting for. How this is weighted would be the judgement of the user. For example, is it more important to take account of the cultural attitudes towards whistle-blowers of the host country, the bank's home country, or the employee's home country? This is an example of how to assess cross-border risks in a dynamic way.

The following risk assessment of C (table 4) is a hypothetical analysis of the risk of an enabler company with multiple risks associated with it, such as a particular bank operating in particular jurisdictions and sectors. While operational experts will have particular knowledge of certain corporations and banks, and a suspicion that they may be being used for tax crimes, this FMEA analysis of the control factor also helps to rationalise knowledge of that suspicion and the factors that may prevent acting on the suspicion successfully - and transfer this knowledge organisationally and to policymakers. This enables those without the experience and expertise related to specific corporations to assess a company under suspicion and encourages rational and evidence-based approach to EU harmonisation of tax crime law.

An example of how this could be evaluated in a multi-dimensional and dynamic application to understand risks to control measures is indicated as follows:

Table 4 Evaluation scheme for assessing risks to C

Risk assessment of enabler company arrangements (this can also be applied to assess the risk in the context of a certain suspicious transaction or financial arrangements being considered).

Rank	Obligations to report suspicious behaviour, in which the company operates[13]	Obligations to maintain secrecy of client's financial transactions (transparency versus secrecy)	Example of whistle-blower risk score (from table 3)	Risk Score
10	No legal obligations to report (e.g. Tax Haven, "Freeport")	Extremely strong commitment to client secrecy		
8-9	Extremely limited legal obligations to report	Fairly strong commitment to client secrecy		
6-7	Limited but existing obligations to report	Committed to client secrecy but with some exceptions		
4-5	Moderate legal obligations to report	Committed to financial transparency but with some exceptions		
2-3	Fairly strong legal obligations to report	Fairly strong commitment to international guidelines on financial transparency		
1	Extremely strong legal obligations to report	Extremely strong commitment to international guidelines on financial transparency		
Enabler company risk score	**4**	**8**	**4.3**	**5.43**

This risk score could be inputted at two stages, as outlined in table 1:

i) The score could be used to assess an action risk, i.e., the extent to which an enabler company risk score denotes or confirms a red flag or, in conjunction with other risks (such as transaction behaviour), denotes sufficient suspicious behaviour to enact operational control measures (C).

ii) The score coujld be used to assess risks to the operational control (C) of a risk, i.e., to what extent does this risk prevent optimum control of other risks and red flags, such as investigating suspicious volumes of cash transactions between two companies?

Taken together, the extent to which these two assessments denote a systemic vulnerability that needs addressing can be ascertained by stakeholders, which can aid in populating the 'suggested next steps' section. Using the risk methodology in this intersecting and dynamic way is optional depending on the context, variety of stakeholders, knowledge and time constraints. The risk methodology is designed to be used to assess risks one at a time (as tables 1 and 2 demonstrate) or in a dynamic and intersecting way (represented by tables 3 and 4). To use it in this dynamic way, users simply have to consider different risks from the evaluation risk tables in Annex 2 and apply them in situations in which their expert knowledge deems appropriate. Overall, this approach is designed to encourage harmonisation across the EU to reduce risk levels.

5. Final remarks

The five key challenges that PROTAX addresses are: i) harmonising prosecution modes of tax crimes, ii) identifying human factors in tax compliance and enforcement, iii) harmonising criminal law on tax offences across the EU, iv) informing future policy and law and iv) informing future research.

To address these challenges, PROTAX is tackling the following topics for end users: comparative analysis of tax and criminal law, tax fraud investigation across borders, information exchange and sharing, human factors and whistle-blowing, asset recovery, insights into interrelation between corruption and tax crimes and a tax crime risk assessment methodology.[26]

The role this risk assessment methodology plays is to produce a framework in which stakeholders can prioritise risks related to the lack of harmonisation across the EU and co-discover ways to resolve them. Bringing stakeholders together to use this risk methodology in training events or knowledge building exercises, as outlined in the use cases section, can aid in doing this. For example, LEA representatives, tax authorities, policymakers and enablers could convene in a day-long workshop to work through the causal chain of risks, from suspicious transaction through to investigation and prosecution, identifying areas of vulnerabilities, risks and brainstorming ways to design out these vulnerabilities and risks by prioritising them and coming up with actions to minimise them. This aligns with the OECD's suggestions for using and embedding their 'Maturity Model' approach to tax crimes within jurisdictions, discussed above. In the case of the PROTAX risk assessment methodology, the stakeholders could be from across the EU, rather than only from within a single jurisdiction and the purpose would be to seek areas in which alignment in operational, institutional, cultural and policy responses to tax crime could minimise the risks inherent in the tax crime eco-system. A version of this risk assessment methodology, along with the other toolkits from WP7, will now be developed further through promulgation efforts in WP8. Feedback will be gained in WP8 on the operability and utility of this risk methodology, as well as specific ideas for new *failure modes*, *control* measures, *effects, evaluation schemes* and *suggested actions* to mitigate the risks we find. The findings from WP8 will be incorporated into the risk methodology in order to tailor it further to ensure it adds maximum value to the tax crime law enforcement environment.

[26] These five key challenges and topics for end users were communicated by the PROTAX consortium to DG Home in response to a request for project information for a 'Community of Users (CoU) in 'Fight against Crime and Terrorism' (FCT) Information Collection' exercise.

6. Annexes

Annex 1a - Risk impact assessment of suspicious transactions

Severity (S)

Likelihood refers to judgement on whether behaviour or event or evidence indicates a tax crime. *Impact* refers to the consequence or seriousness of the tax crime to which it alludes.

	Likelihood this red flag indicates tax crime (failure mode)	Very Low	Low	High	Very High
Impact / seriousness of consequences	Very low	1	2/3	4/5	6/7
	Low	2/3	4/5	6/7	8/9
	High	4/5	6/7	8/9	10
	Very High	6/7	8/9	10	10

Annex 1b - Risk impact assessment of control measures

Severity (S)

Likelihood refers to judgment on whether the identified vulnerability is preventing control of the risk (suspicious transaction / red flag) identified.

Impact refers to the seriousness of the effect this may have on the ability to control the suspicious transaction / behaviour

	Likelihood this vulnerability is preventing control of potential tax crime (failure mode)	Very Low	Low	High	Very High
	Very low	1	2/3	4/5	6/7
	Low	2/3	4/5	6/7	8/9

Impact / seriousness of consequences	High	4/5	6/7	8/9	10
	Very High	6/7	8/9	10	10

Annex 1c - Evaluation scheme for control measures

Control (C)

10	No control measures in place.
8-9	Control measures in place but highly ineffective.
6-7	Limited control measures, meaning successful control of risk is probably unlikely on most occasions.
4-5	Moderate control measures but with some deficiencies, meaning an ability to control the risk exists, but the success of the control measures is not guaranteed.
2-3	Fairly good control measures in place, meaning risk can more often than not be controlled successfully.
1	Extensive, robust and comprehensive control measures in place to control the risk identified.

Annex 2 – Risk tables (vulnerabilities)

PROTAX has identified key vulnerabilities and discrepancies in the EU tax crime law enforcement environment that pose a risk to controlling suspicious transactions and tax crimes. These were discovered during the extensive work carried out in WP 1 – 6, which included focus groups, case studies and comparative analysis of legal regimes. These key areas are set out in the draft risk tables below. These tables are to be populated fully by users of the risk methodology, as the professional judgment of the extent and severity of the risk, and measures to overcome that risk, can be unique to certain circumstances, organisations and MS. However, for others, a stronger input from PROTAX is possible to give a lead on the specific nature those risks pose for tax crime and its detection.

Key vulnerabilities producing risks are:

Scope and definitions of tax crimes
Threshold of tax crimes
Sanctions for tax crimes
Legal liability for tax crimes
International co-operation on criminal matters
Information sharing
Whistle-blower treatment
Obligations to report suspicious financial behaviour
Obligations to maintain secrecy of client's financial transactions (transparency versus secrecy)
Resource constraints

The control measures that are in place will differ depending on context and on the user of the risk methodology and can be added by the user to assess whether they are sufficient. For example, two LEAs may happen to have a good working relationship that can overcome the issue of information sharing across jurisdictions, but others may not. The actions / recommendations will also be varied depending on circumstances, however, recommendations based on the knowledge gained in PROTAX WP 1 – 6 have been added into these columns as an example. Because PRORAM can be used as a training tool, and as a way for a variety of stakeholders to come together to 'design out' failure modes, risks for different stakeholders, such as enablers and LEAs, can be included in same table where appropriate. The risk tables that follow assess the key vulnerabilities within the tax crime law enforcement eco-system (level 2). These tables can be used dynamically in response to different threats and risks identified in level 1. For example, a suspicious transaction that involves financial arrangements spanning multiple jurisdictions contains variables that do not pertain to localised suspicious transaction involving only one jurisdiction. In such circumstances the assessment of risk will differ. For each risk table below, PROTAX has offered a description of the vulnerability identified, populated the table with some basic examples to encourage brainstorming by users, and provided a descriptive evaluation table to guide assessment and scoring of risk.

Guidance for user

For each risk table:

1. Consider the failure mode (F) described in **column one**.

2. Use the evaluation scheme (E) table below the risk table to populate **column two.**

3. Discuss and describe the effects that each risk table failure mode may have, and input this into **column three.**

4. Use annex 1a to populate **column four**. This assesses the severity (S) of the failure mode by assessing the likelihood that the failure mode will produce the effects that you have described, and the impact of those effects should they happen.

5. Describe control measures (C) that are already in place (if any) to address the failure mode under consideration. Score the effectiveness of these control measures by using annex 1c and input this into **column five**

6. Add E + S + C to produce a risk priority number (RPN) in **column six.** This allows you to quantify and assess which risks should be prioritised for treatment (you can go back and re-adjust these scores if necessary having filled out other failure mode risk tables).

7. Discuss and describe actions and recommendations that could be implemented to treat the risk and lower the RPN, then input them into **column seven**.

1. Scope and definition of tax crimes – risk table

Taxonomies of criminalised conduct related to tax crimes differ across Member State jurisdictions. For example, no uniform definition of tax fraud (or even VAT fraud) could be found across Member States. Only by assessing other objective elements of the criminal offence is it possible to establish criminal liability for VAT fraud in all countries[27].

This creates risks for enablers, policy makers and LEAs, as potential vulnerabilities and loopholes are produced by different categorisations and typologies of tax crime and fraud, which can be exploited by tax criminals when conducting their financial affairs across different jurisdictions.

Potential Failure Mode	**Evaluation scheme for F risk**	**Effects (examples)**	**Severity (likelihood failure mode produces effect, + impact)**	**Control (measures in place to overcome F)**	**Risk priority number (RPN)**	**Actions/ recommendations (examples)**
Unclear or diverging definitions of tax crime	**[Input score]** Use evaluation scheme table below	Inability to investigate / prosecute a tax crime Customer / client exploits this discrepancy to commit tax crime in different jurisdiction through your company	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Change MS policy on tax crime definitions Liaise with partner LEAs in different jurisdictions to align operational definition for tax crimes Align a working typology between different MS LEAs for specific investigation Refuse to work with customer exploiting this discrepancy

[27] Umut Turksen, Reinhard Kreissl, Emanuel Blumenschein, Franz Reger, Ana Djakovic, Adam Abukari, PROTAX, Deliverable D3.2, 'A Comparative Analysis of Tax Crimes in the European Union', 08.07.2020, [p60]

Table: Evaluation scheme for scope and definition of tax crime

Rank	Scope and definition of tax crime between MS
10	No alignment between MS on scope and definition of tax crime
8-9	Scope and definitions of tax crime vary widely
6-7	Limited alignment of scope and definition
4-5	Moderate differences in scope and definition
2-3	Scope and definition quite similar
1	Scope and definition aligned between MS

2. Threshold of Tax Crimes – risk table

Thresholds for criminalising tax crimes differ across Member State jurisdictions. Such thresholds are in fact an integral part of the definition of tax offences because ‘they allow tax offenders to define whether their acts constitute a criminal offence. Therefore, some behaviours can be considered an offence only if they reach a threshold’.[28] Further complications exist in regard to how criminalised thresholds are determined. For example, according to Austrian law, the threshold for criminalisation relates to the overall sum of taxes evaded, whereas Greek law calculates the threshold according to each kind of tax separately for each fiscal year.[29] Consequently, these discrepancies and variations create risks for enablers, policy makers and LEAs as potential vulnerabilities and loopholes are produced that tax criminals can exploit or lower their own risk of criminalisation.

Potential Failure Mode (F)	**Evaluation scheme for F risk**	**Effects (example)**	**Severity (likelihood failure mode produces effect, + impact)**	**Control (measures in place to overcome F)**	**Risk priority number (RPN)**	**Actions/ recommendations / suggested next steps**
Diverging thresholds for tax crime between jurisdictions	**[Input score]** Use evaluation scheme table below	Inability to investigate / prosecute	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Liaise with partner LEAs in different jurisdictions to align a working threshold for investigation Change MS policy on tax thresholds
		Customer / client exploits this discrepancy in thresholds to commit tax crime in different jurisdiction through your company				Refuse to work with customer

[28] *Ibid*. [p. 60]

[29] *Ibid*. [p. 66]

Table: Evaluation scheme for diverging thresholds on tax crime

Rank	Diverging tax crime thresholds between jurisdictions
10	No alignment in thresholds of tax crime
8-9	Thresholds for tax crime vary widely
6-7	Limited alignment of thresholds
4-5	Moderate differences in thresholds
2-3	Thresholds quite similar
1	Thresholds aligned
Risk ranking	

3. Sanctions for tax crimes – risk table

The question here for risk assessment is, does the jurisdiction provide sanctions that are effective, proportionate and dissuasive? For example, in the case of VAT fraud, sanctions for VAT fraud defined under Articles 3(2) and 2(2) of PIF Directive (i.e., committed in more than one state and involving damage of at least EUR 10.000.000) are expected to be considerable.[30] These offences have to be punished by a maximum penalty of at least four years of imprisonment, according to this directive. The penalty in each Member State should be effective, proportionate and dissuasive, or the Member State is in danger of being in breach of the PIF Directive. However, this is sometimes not the case.

The effectiveness of sanctions can be evaluated in the table below (E) by considering a combination of their severity, swiftness and the probability of detection. With this in mind, could there be room for improvement in sanctions?

Potential Failure Mode	**Evaluation scheme for F risk**	**Effects (example)**	**Severity (likelihood failure mode produces effect, and impact)**	**Control (measures in place to overcome F)**	**Risk priority number (RPN)**	**Actions/ recommendations**
Ineffective and non-dissuasive sanctions regime	**[Input score]** Use evaluation scheme table below	Low compliance rates Client uses jurisdiction to commit tax crime because risk for them is lower	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Increase sanctions Do not operate in jurisdiction

[30] Franz Reger., Ana Djakovic., Umut Turksen., Donato Vozza., Adam Abukari., 'Report on comparative legal and institutional analysis', PROTAX, Deliverable D3.1, May 2020.

Table: Evaluation scheme for sanctions for tax crime (E)

Rank	Sanctions for tax crime
10	Very light sanctions, slow process of investigation / prosecution and low probability of detection producing highly ineffective and non-dissuasive sanctions regime
8-9	Ineffective and non-dissuasive sanctions regime for tax crime
6-7	Relatively ineffective and non-dissuasive sanctions regime for tax crime
4-5	Moderately effective and dissuasive sanctions regime for tax crime
2-3	Fairly effective and dissuasive sanctions regime for tax crime.
1	Severe sanctions with swift process and high probability of detection, producing highly dissuasive sanctions regime for tax crime

4. Legal liability for tax crimes in Member States – risk table

PROTAX D3.1 indicates that there are countries that include a legal framework on the liability of legal entities for tax crimes and others that do not include it or limit the scope only to certain tax crimes. The nature of the liability is different in various countries (criminal, administrative, and *tertium genus*. The sanctions applicable on legal persons are fines in the first instance, and, in some countries, other measures such as banning them from tax benefits or future contracting with public authorities.[31] The differential nature of legal liability across and within Member States may create vulnerabilities that undermine a robust tax crime law enforcement environment. This may also create an 'environment' in which tax crime flourishes, the effects of which could be to make one jurisdiction more attractive than others, undermining competition law and giving unfair advantage to certain localities as more money (both dirty and clean) is attracted to it.

Potential Failure Mode	**Evaluation scheme for F risk**	**Effects (example)**	**Severity (likelihood that failure mode produces effect, + impact)**	**Control (measures in place to overcome F)**	**Risk priority number (RPN)**	**Actions/ recommendations**
Ineffective legal liability regime in MS	**[Input score]** Use evaluation scheme table below	Ineffective compliance, deterrence Unable to prosecute Attracts tax criminal's business, undermining fair competition Client moves money through jurisdiction without sufficient justification	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Align legal liability Do not operate in jurisdiction

[31] *Ibid*. [p. 159]

Table: Evaluation scheme for sanctions for tax crime

Rank	Legal liability for tax crime
10	Very ineffective and / or confusing legal liability regime
8-9	Ineffective and / or confusing legal liability regime
6-7	Legal liability regime has lots of areas that are ineffective with some exceptions
4-5	Legal liability regime has some areas of ineffectiveness
2-3	Fairly comprehensive, targeted and clear legal liability regime
1	Very comprehensive, targeted and clear legal liability regime

5. International cooperation in criminal matters – risk table

As discovered in PROTAX D3.1,[32] international cooperation in criminal matters is a key instrument of the European Union to counter tax offences. Several Council Framework Decision and Directive contain specific provisions regulating cooperation where issuing and executing states do not provide for the same type of taxes. Recently, PIF Directive introduced provisions to strengthen cooperation between MS and the EU for assistance pertaining to VAT fraud. The effectiveness of these provisions are under studied, and as such require attention in the development of the PROTAX toolkits. The extent to which cooperation can be modelled as risk is the topic of this table.

Potential Failure Mode	Evaluation scheme for F risk	Effects (example)	Severity (likelihood failure mode produces effect, and impact)	Control (measures in place to overcome F)	Risk priority number (RPN)	Actions/ recommendations
Lack of cooperation between MS LEAs and tax authorities	**[Input score]** Use evaluation scheme table below	International VAT fraud goes undetected Client uses discrepancy to commit tax crime	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Break silos Identify and contact opposite number in MS LEA EU directive / policy change on cooperation. Do not operate in jurisdiction

[32] Ibid.

Table: Evaluation scheme for international cooperation on criminal matters

Rank	International cooperation on criminal matters
10	No international cooperation
8-9	Ineffective cooperation
6-7	Cooperation exists but is limited
4-5	Cooperation in some areas but lacking in others.
2-3	Fairly effective cooperation
1	Very effective cooperation going above and beyond international and EU guidance

6. Information sharing – risk table

Information sharing across borders, agencies and jurisdictions is key to the tax crime investigation eco-system. However, through the PROTAX focus groups and other work in WP 1 – 6 we have discovered this to be failing in many areas. Some LEAs have good working relationships with their counterparts in other jurisdictions, but this is ad-hoc and unpredictable. Europol have identified information as a key area for improvement, and FIU.net, a platform to share information about tax crime perpetrators without divulging personal details that may identify them in contravention of local laws, could play a part in improving information sharing. Statistical alignment of information to improve tax crime law enforcement is also key. For example, PROTAX discovered in WP5 that information on asset recovery from tax crimes is either not recorded at all in some jurisdictions or is not shared with the relevant authorities when it is recorded. Without this information operational learning is undermined, meaning, for example, that investigations into companies that may have already been subject to asset seizure (but not necessarily criminal sanctions) are conducted without that knowledge.

Potential Failure Mode	Evaluation scheme for F risk	Effects (example)	Severity (likelihood failure mode produces effect, and impact)	Control (measures in place to overcome F)	Risk priority number (RPN)	Actions/ recommendations
Lack of information sharing between different MS LEAs and/or **tax authorities**	**[Input score]** Use evaluation scheme table below	International VAT fraud goes undetected Client uses discrepancy to commit tax crime	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Engage FIU.net Identify and contact opposite number in MS LEA EU directive / policy change on information sharing Do not operate in jurisdiction

Table: Evaluation scheme for information sharing

Rank	Information sharing
10	No information sharing
8-9	Ineffective information sharing
6-7	Information sharing occurs but is limited
4-5	Information sharing in some areas but lacking in others.
2-3	Fairly effective information sharing
1	Very effective information sharing relationship established.

7. Whistle-blower treatment – risk table

Directives to protect whistle-blowers exist – such as the 'Directive on the Protection of persons reporting on breaches of Union law', which should be in force in EU Member States by 17 December 2021**.** This EU whistle-blower directive provides new measures on the protection of whistle-blowers who disclose a violation of the EU law, including specific aspects related to tax.[33] However, while legal requirements to protect whistle-blowers have been adopted at the EU level, PROTAX has discovered that the grey area of human, cultural and institutional factors interact to impact on whistle-blowers in different ways. These are modelled as risk in the following table, which can be added to the control risk of any given red flag issue.

Potential Failure Mode	Evaluation scheme for F risk	Effects (example)	Severity (likelihood failure mode produces effect, + impact)	Control (measures in place to overcome F)	Risk priority number (RPN)	Actions/ recommendations
Lack of whistle-blower protection (legal, corporate, cultural)	**[Input score]** Use evaluation scheme table below	International VAT fraud goes undetected Corporate client hostile to whistle-blowing	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Enforce EU directive / policy change on whistle-blower protection Develop ways to change cultural attitudes to whistle-blowers Embed corporate protection for whistle-blowers Public campaign about the benefits of whistle-blowing Do not work with client

[33] *Ibid.*

Table Evaluation scheme for whistle-blower treatment

Rank	Corporate attitudes to whistle-blowers	Legal protection of whistle-blowers	MS cultural attitudes to whistle-blowers	Evaluation score
10	A demonstrably hostile corporate environment for whistle-blowers	Prosecution of whistle-blowers highly likely	Hostile (“snitch”, “grass” etc)	
8-9	A difficult corporate environment for whistle-blowers	Prosecution of whistle-blowers quite likely	Culturally hostile but acceptable in certain circumstances	
6-7	No corporate support	Prosecution of whistle-blowers possible	Ambiguous but generally negative	
4-5	Some minimal corporate support	Minimal legal protections for whistle-blowers	Ambiguous but generally positive	
2-3	Corporate support but without specific and / or robust corporate whistle-blower policy	legal protections for whistle-blowers	Generally positive attitudes to whistle-blowers	

1	Corporate support embedded within robust company policy	Robust legal protections for whistle-blowers	Positive attitudes to whistle-blowers (“public champions”, “heroes” etc)
Whistle-blower risk score*			

*****To obtain whistle-blower evaluation score calculate the mean average of the three individual whistle-blower risk ratings and put in the bottom row of ‘evaluation score’ column.

8. Obligations to report suspicious financial behaviour

Discrepancies between and amongst EU member states on the legal obligations placed on people to report suspicious financial behaviour operating within their jurisdiction - including the development of freeports, and between EU member states and external countries – present potential vulnerabilities in the tax crime law enforcement eco-system.

Potential Failure Mode	Evaluation scheme for F risk	Effects (example)	Severity (likelihood failure mode produces effect, + impact)	Control (measures in place to overcome F)	Risk priority number (RPN)	Actions/ recommendations
Obligations to report suspicious financial behaviour	**[Input score]** Use evaluation scheme table below	International VAT fraud goes undetected Corporate client operating in suspect jurisdiction	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Policy changes on secrecy laws Public campaign on alignment (or against egregious examples like freeports) Do not work with client Refuse to work in jurisdiction Engage with Tax Justice Network's secrecy index[34] to assess and list jurisdictions to avoid.

[34] Tax Justice Network (TJN), Financial secrecy index, 2020 https://fsi.taxjustice.net/en/ .

Table: Evaluation scheme for Secrecy

Rank	Secrecy
10	No legal obligations to report (eg Tax Haven, “Freeport”)
8-9	Extremely limited legal obligations to report
6-7	Limited but existing obligations to report
4-5	Moderate legal obligations to report
2-3	Fairly strong legal obligations to report
1	Extremely strong legal obligations to report

9. **Obligations to maintain secrecy of client's financial transactions (transparency versus secrecy)**

Institutional, corporate and cultural factors within which secrecy prevails inside financial institutions, corporations and client's financial affairs is an issue across the EU and an example of the 'grey area' of tax crime law and human factors impacting the effectiveness of tax crime law. PROTAX discovered that the tension between the secrecy of a client's financial affairs on the one hand, and legal or even ethical obligations to report suspicious behaviour on the other, generate risks and undermines effective decision making for enablers and other professionals with reporting duties.[35] In this context, it is the staff members of relevant organisations (banks, tax authorities, notaries, tax consultants, etc.) who also represent individual sources of risk related to how they decide to behave. This is the human factor emphasised by PROTAX and elaborated in D3.2[36]

Potential Failure Mode	Evaluation scheme for F risk	Effects (example)	Severity (likelihood failure mode produces effect, + impact)	Control (measures in place to overcome F)	Risk priority number (RPN)	Actions/ recommendations
Obligations to maintain secrecy of client's financial transactions (transparency versus secrecy)	**[Input score]** Use evaluation scheme table below	International VAT fraud goes undetected Corporate client maintaining unjustifiable secrecy of financial affairs	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Policy changes on corporate secrecy laws Encourage whistle-blowers Public campaigning on corporate transparency Do not work with client Refuse to work with secretive corporations and financial institutions

[35] Matthew Hall, David Wright, Reinhard Kreissl, Umut Turksen, 'A framework for the ethical, privacy and social impact assessment of tax crimes', PROTAX, deliverable D6.2, 31.01.2020.

[36] Umut Turksen, Reinhard Kreissl, Emanuel Blumenschein, Franz Reger, Ana Djakovic, Dr Adam Abukari, PROTAX, Deliverable D3.2, 'A Comparative Analysis of Tax Crimes in the European Union', 08.07.2020.

Table: Evaluation scheme for corporate secrecy

Rank	Corporate secrecy
10	Extremely strong commitment to client secrecy
8-9	Fairly strong commitment to client secrecy
6-7	Committed to client secrecy but with some exceptions
4-5	Committed to financial transparency but with some exceptions
2-3	Fairly strong commitment to international guidelines on financial transparency
1	Extremely strong commitment to international guidelines on financial transparency

10. Resource constraints – risk table

During the PROTAX focus groups resource constraints were highlighted repeatedly as an important variable in the successful investigation and prosecution of tax crimes. Limits on personnel, technologies and time means that LEAs and tax authorities must discriminate between different tax crimes and make hard choices about which tax crime investigation to pursue. Tax crimes are often complex and difficult to prosecute, and in combination with resource constraints this produces the perceived need among some LEAs and tax authorities to pursue 'sweetheart deals' with large corporations, because the resources necessary to fully prosecute complex cases are lacking. Resource constraints also impact upon law enforcement. For example, PROTAX discovered that tax criminals were more likely to choose urban centres with more pressures on LEAs and tax authorities over quieter jurisdictions where the likelihood of detection would be higher. This obviously presents a risk for tax crimes in those areas of resource constraints.

Potential Failure Mode (F)	**Evaluation scheme for F risk (E)**	**Effects (example)**	**Severity (S) (likelihood failure mode produces effect, + impact)**	**Control (C) (measures in place to overcome F)**	**Risk priority number (RPN)**	**Actions/ recommendations**
Insufficient resources to successfully pursue complex tax crime	**[Input score]** Use evaluation scheme table below	Tax criminals choose jurisdiction to commit tax crime	**[Input score]** Use annex 1 to assess risk.	**[Input description and score]** Describe control measures and assess effectiveness by using annex 1c	**[Input number]** E + S + C	Provide more resources for LEAs and tax authorities in areas under pressure of tax crimes
		Corporate client registers business in area of tight resource constraints without logical financial justification				Seek plausible financial justification / clarification for client registering businesses in jurisdiction with resource constraints

Table: Evaluation scheme for resource constraints

Rank	Resource constraints
10	Extremely limited resources, without the necessary personnel, time or technology, meaning most suspected tax crimes are not subject to investigation.
8-9	Limited resources, with serious gaps in personnel, time or technology, meaning a lot of suspected tax crimes are not subject to investigation.
6-7	Resources are sufficient in some areas but importantly lacking in others, meaning many complex tax crimes are not investigated as well as they could be.
4-5	Department / geographical area is resourced sufficiently, but with some important gaps, meaning some complex tax crimes are investigated fully and impartially but others are not.
2-3	Fairly well-resourced department / geographical area with the sufficient personnel, time and technology to pursue most complex tax crimes fully and impartially.
1	Extremely well-resourced department / geographical area, with sufficient personnel, time and technology to pursue all complex tax crimes fully and impartially.

Annex 3 – Questions indicating a suspicious behaviour / transaction / financial arrangement (red flags)[37]

The important factor for enablers and professionals is to question the rationale and logic behind the transactions and financial behaviour they are considering. It is also the case that professionals and experts with more industry knowledge will be able to produce their own questions to alert them to suspicious behaviour. However, these questions have been designed as a guide, and in the first two tables include questions that may specifically indicate a tax crime developed in conjunction with PROTAX LEA partners, rather than only indicating an undefined suspicious transaction. It is important to note that these questions alone do not necessarily indicate definite suspicious behaviour, and the expert user must use their knowledge of the logic of the transaction or behaviour when making a judgment. These questions have been produced in conjunction with LEA and FIU partners in PROTAX, information from the PROTAX WP 1 – 6 and research of common industry KYC protocols and questions.

Questions concerning types of suspicious activities, arrangements and transactions **that may specifically indicate a tax crime**
• Does this company have no or only a few employees?
• Has this company recently replaced a member of the management board?
• Has this company just been set up?
• Are this company's wages lower than average?
• Is there no logical or economic explanation for the transactions (i.e. the chain of companies is too long)?
• Is the same pattern of transactions being carried out with different companies in succession?
• Has the money moved through several countries?
• Are alternative payment platforms used for money transfers?
• Has money been transferred to another country in a different jurisdiction with the explanation 'loan' or 'agreement'?
• Does the company 'unnecessarily' span jurisdictions? For example, registered in one country, bank account opened in another, and board member located in a third?

[37] These questions were co-created with PROTAX LEA and FIU partners and through research into KYC guides and protocols that exist across the industry, FIU advice to professionals with reporting duties and guidance from anti-money laundering bodies, such as the Wolsberg group and the Financial Action Task Force. Advice and guidance on red flags discovered during this research have been turned into the questions in this section. Sources for these questions include: PWC, Know Your Customer: Reference guide, 2016, https://www.pwc.co.uk/assets/pdf/kyc-qrg-final-interactive.pdf; Financial Action Task Force, Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, June 2013, http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf; The Wolfsberg Group, Wolfsberg Guidance on Customer Tax Evasion, 2019, https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20Guidance%20on%20Customer%20Tax%20Evasion.pdf; Belize FIU, Types of Suspicious Activities or Transactions, 2020, http://fiubelize.org/types-of-suspicious-activities-or-transactions/ .

Questions assessing a company's tax compliance, reliability and tax behaviour[38].

Answering these questions in the positive indicates further due diligence or investigation is required.

- Does the company have arrears or is it subject to insolvency proceedings?
- Has the company failed to submit all necessary declarations?
- Is there at least two punishments for tax and customs misdemeanours in force against this company and/or one or more punishments for criminal offences?
- Have tax proceedings and/or control activities carried out over the last 12 months have revealed significant errors in the submitted data?
- Does someone involved in a key position in the company have arrears and/or that person is subject to insolvency proceedings and/or has received a prohibition on business or prohibition to engage in enterprise or companies related to the person have unpaid tax arrears?
- Are there are deficiencies in how a company has declared expenses unrelated to business and fringe benefits?
- Are there are significant deficiencies in how a company has declared payments of the previous period of taxation?
- Does the company have significant deficiencies in the data in the employment register?
- Are there significant deficiencies in how a company has declared acquisition of goods and services?
- Are there are significant deficiencies in how a company has declared sale of goods and services?

Questions about company Formation and management

Suspicious circumstances relating to the customer's behaviour in this context include:

- Have companies been purchased which have no obvious commercial purpose?
- Do sales invoice totals exceed known value of goods?
- Does this customer appear uninterested in 'legitimate' tax avoidance schemes?
- Does the customer pay over the odds or sell at an undervaluation?

[38] This particular table of questions was adapted from feedback offered on this risk assessment methodology by the Estonian Tax and Customs Board (ETCB) at one of the first WP8 workshops. The questions included here are influenced by how the ETCB calculates company's tax behaviour ratings.

- Does the customer make unusually large cash payments in relation to business activities which would normally be paid by cheques, banker's drafts etc?

- Has this customer transferred large sums of money to or from overseas locations with instructions for payment in cash?

- Does this customer have numerous bank accounts and pay cash into all those accounts which, if added together, would amount to a large overall sums of money?

Questions concerning new company or clients

The following situations should result in additional enquiries when engaging with a new company or client.

- Is verification of identity proving unusually difficult, or is this customer reluctant to provide details?
- Does this corporate client produce difficulties and unnecessary delays in obtaining copies of company accounts?
- Is this client using your company with no discernible reason e.g. could they just as easily deal with a company closer to where they live or could the services they are seeking be better served by another company?
- Are there any transactions in which the counterparty to the transaction is unknown?

Questions relating to suspicious circumstances of groups of companies

- Are subsidiaries involved in this customer's financial arrangements that have no logical purpose?
- Is there a company involved that makes substantial losses on an ongoing basis?
- Do complex group structures exist without any apparent cause?
- Are the group structures involved for tax purposes apparently uneconomic?
- Is there a frequent change in the shareholders and directors?
- Are there unexplained transfers of significant sums of money through several bank accounts?
- Are several currencies without reason in the same bank accounts?

Questions related to potential money Laundering

While money laundering can be a sign of many underlying predicate offences, tax criminals often need to launder their proceeds and turn 'dirty' cash into 'clean' cash to hide their tracks and get their money moved to where it is more difficult to detect.

Money-laundering through accounts

- Does this customer wish to maintain a number of accounts which do not appear consistent with the type of business they run, for example, using nominees in transactions?
- Does the customer pay cash into numerous accounts which, while taken in isolation is not a large amount, but taken together add up to a large amount of cash overall?
- Does the account either receive or disburse large amounts of money that apparently do not have a legitimate or obvious purpose to the account, account holder or business?
- Has this customer provided minimal or fictitious information, or have they provided information that is expensive and troublesome for the institution to verify?
- Does this customer have several accounts within the same geographical locality, city or jurisdiction?
- Does this customer take cash out regularly on the same day as the same amount of cash was credited to their account?
- Have large withdrawals been suddenly made from a previously 'dormant' account?
- Do a company's representatives seem to want to avoid face to face contact with the bank?
- Does the customer decline to provide information that would make the customer eligible for more beneficial banking services when offered?
- Do large numbers of individuals make payments into the same account without a logical or adequate explanation?

Money-laundering using cash

- Have large deposits been made by a company, or an individual, whose ordinary business activities would commonly involve cheques or other financial instruments?
- Have cash deposits of any individual or business suddenly increased without apparent cause? If so, are these deposits subsequently transferred out of the account to a destination not normally associated with the customer?
- Has the customer used numerous credit slips to deposit cash so that the total of each deposit is unremarkable, but the total of all the credits is significant?

- Does this customer constantly pay in or deposit cash to cover requests for money transfers, bankers drafts or other marketable money instruments?
- Is this customer seeking to exchange large quantities of low denomination notes for higher denominations? Does this happen regularly?
- Does this customer frequently exchange cash into other currencies?
- Does this customer deposit large amounts of cash using night safe facilities, thereby avoiding face to face contact with bank staff?
- Has one branch had a great deal more cash transactions than usual?
- Does this customer’s deposits contain counterfeit notes?

Money-laundering offshore

- Does the customer use letters of credit to move money between countries where such activity is inconsistent with the customer’s ordinary behaviour and financial interests?
- Is the customer building up large balances that are inconsistent with the turnover of the business in question?
- Are there any unexplained fund transfers by customers or foreign currency drafts?
- Have there been frequent requests for traveller’s cheques or foreign currency drafts or other negotiable instruments to be issued?
- Is there a frequent paying in of traveller’s cheques or foreign currency drafts particularly if originating from overseas?

Money-laundering involving financial institution employees and agents

- Has there been any changes in employee characteristics, (e.g. suddenly opulent lifestyles or, visa versa, avoiding taking holidays or making purchases that were previously common place for this customer)?
- Has there been any changes in employee or agent performance, (e.g. a salesman has a sudden and unexpected upturn in performance)?
- Is the identity of the ultimate beneficiary undisclosed and is this an abnormal occurence for the type of company in question?

Money-laundering through lending

- Has the customer repaid a ‘problem loan’ unexpectedly?
- Has the customer requested to borrow against assets held by an institution or a third party, where, either, the origin of the assets in not known, or, the assets are inconsistent with the customer’s standing?
- Has the customer requested for an institution to arrange finance where the source of the customer’s financial contribution to deal is unclear, particularly where property is involved?

Questioning the use of Intermediaries

There are many legitimate reasons for a client's use of an intermediary. However, the use of intermediaries introduces additional parties into a transaction, and this can increase complexity, anonymity and secrecy.

The key factor here is to be alert to **unnecessary or illogical** use of an intermediary in the transaction.

Question: In your judgment is the use of an intermediary in this transaction unnecessary?

Abnormal and illogical transactions

The aim of the tax criminal is often to introduce multiple layers in any transaction or financial arrangement to increase opacity of their financial dealings. This may mean that money will pass through different entities and institutions. Again, the key factor to consider is whether any apparently abnormal patterns are illogical or make no financial sense.

Questions about the logic or financial sense of a transaction

- Has there been a large number of security transactions across a number of jurisdictions?
- Are transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates?
- Have securities been bought or sold with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request?
- Have low grade securities purchased in an overseas jurisdiction been sold locally and with the profits high grade securities have been purchased?
- Have a number of transactions been made by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account?
- Is there any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading; early cancellation, especially where cash had been tendered or their fund cheque is to a third party?
- Has there been a transfer of investments to apparently unrelated third parties?
- Are there any transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices?

Questions to uncover suspicious types of secrecy

A customer wanting to maintain a level of privacy in their financial affairs is understandable. However, the following may imply suspicious secrecy and should give rise to further enquiries.

- Is there an excessive use of nominees?
- Do sales invoice totals exceed known value of goods?
- Is the customer performing 'execution only' transactions?
- Does the customer use a client account rather than paying for things directly?

- Does the customer use a mailing address that is not their own address?
- Is there unwillingness on behalf of the customer to disclose the source of their funds?
- Is there an unwillingness on behalf of the customer to disclose the identity of ultimate beneficial owners?

Annex 4 – Blank risk assessment tables

Annex 4a – risk assessment table for level 1

Potential Failure Mode (F)	**Effects (example)**	**Severity (S) (likelihood failure mode produces effect, + impact)**	**Control (C) (measures in place to overcome F)**	**Risk priority number (RPN)**	**Actions/ recommendations**

Annex 4b – risk assessment table for level 2

Potential Failure Mode (F)	Evaluation scheme for F risk (E)	Effects (example)	Severity (S) (likelihood failure mode produces effect, + impact)	Control (C) (measures in place to overcome F)	Risk priority number (RPN)	Actions/ recommendations