FATF • GAFI

Financial Action Task Force

Groupe d'action financière

MONEY LAUNDERING & TERRORIST FINANCING RISK ASSESSMENT STRATEGIES

18 June 2008

TABLE OF CONTENTS

ACRONYMS

AML	*Anti-money laundering*
CDD	*Customer due diligence*
CFT	*Combating the financing of terrorism*
DNFBPs	*Designated non-financial businesses and professions*
FATF	*Financial Action Task Force*
FI	*Financial institution*
FIU	*Financial intelligence unit*
FSRB	*FATF-style regional body*
IMF	*International Monetary Fund*
LEA	*Law enforcement agency*
ML	*Money laundering*
RBA	*Risk-based approach*
SAR	*Suspicious activity report*
SSI	*Strategic surveillance initiative*
STR	*Suspicious transaction report*
TF	*Terrorist financing*
WGTYP	*Working Group on Typologies*
WB	*World Bank*

INTRODUCTION

1. Understanding the sources and methods of money laundering and terrorist financing in a jurisdiction is essential for competent authorities to develop and implement an effective anti-money laundering/counter-terrorist financing (AML/CFT) programme. A national money laundering/terrorist financing (ML/TF) risk assessment should be considered the foundation for setting AML/CFT policy priorities and resource allocation.

2. The purpose of this report is to provide information on developing a national ML/TF risk assessment. There are obvious similarities and differences between money laundering and terrorist financing, but the risks of both are often assessed and managed using the same information flows between public and private sector institutions.[1]

3. The Financial Action Task Force (FATF) typology report, *Terrorist Financing*, published in February 2008 notes: "The application of the FATF 40 Recommendations and 9 Special Recommendations provides a solid basis upon which to gather financial information. Leveraging this financial information with wider information on counterterrorism, including intelligence, at a national level may prove to be the most effective use of financial information in identifying terrorist activity."[2]

4. The terminology used in this paper as well as the risk management principles and procedures that are presented draw heavily on the June 2007 FATF paper, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing* (RBA paper).[3] The RBA paper defined a "risk management process for dealing with money laundering and terrorist financing" that encompasses *i)* recognising the existence of risks; *ii)* undertaking an assessment of the risk(s); and *iii)* developing strategies to manage and mitigate the identified risks.[4] This paper offers methodologies for undertaking the risk assessment portion of that framework at the national level.

5. Although depth of coverage may differ, a national ML/TF risk assessment is a process that typically presents information on:

- The nature and scale of ML/TF and related predicate crimes (*i.e.* the threat).
- Weaknesses in AML/CFT systems and controls and other features of a jurisdiction that make it attractive to money launderers and terrorist financiers (*i.e.* the vulnerability).[5]

6. The purpose of a national ML/TF risk assessment is to identify money laundering and terrorist financing methods across a jurisdiction and to determine how often those methods are used, how

[1] Although intelligence sources provide insights into terrorist financing activities, that information and information related to money laundering gathered from law enforcement flows to the private sector as risk management guidance, advisories, and targeted economic sanctions. The private sector also is alerted to risks regarding specific individuals, entities, and transactions through information requests received from law enforcement. Relevant ML/TF information flows the other way as well, through currency and transaction reporting from financial institutions required to file such reports.

[2] FATF (2008).

[3] FATF (2007a).

[4] *Ibid*.

[5] There are currently no standard definitions used internationally within the AML/CFT context for the terms risk, threat, and vulnerability. This project identifies concepts linked to these terms in order to promote a consistent approach by countries, but does not go so far as to suggest precise definitions for adoption by the international community. Having a clear understanding of what the concepts mean, however, will assist countries when establishing the terms of reference and scale of ambition when conducting a national ML/TF assessment.

effective they are in moving illicit funds, and whether there are gaps in the AML/CFT systems and controls.

7. A national ML/TF risk assessment should be regarded as "fundamental background information" to assist supervisors, law enforcement authorities, the financial intelligence unit (FIU), and financial institutions.[6] This requires that competent authorities periodically renew their awareness of current money laundering and terrorist financing methods and reassess the effectiveness of established safeguards.

8. The ML/TF risk assessment process should inform a consideration of whether current laws are sufficient to address new threats, and whether current methods of supervision and enforcement are adequate. Where the law is inadequate, there is vulnerability. Where the law is adequate, but supervision and examination are weak law enforcement will be overwhelmed. Where law enforcement is weak, the law has little deterrent effect.

9. Conducting a risk assessment should be useful to policymakers in identifying AML and CFT priorities. "The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention."[7] Assessments should be tied to strategic planning and linked to specific actions.

10. In addition to identifying high priority ML/TF risks at the national or jurisdictional level, aggregating risk assessments across jurisdictions will help to identify priority concerns at the international level. To support the goal of producing a global threat assessment, the February 2008 FATF plenary initiated the Strategic Surveillance Initiative (SSI). The SSI process includes aggregating existing national ML/TF risk assessments, surveying FATF and FATF-style regional body members regarding emerging trends and high priority ML/TF risks, fact-finding by the FATF Secretariat, and discussion in the FATF Working Group on Typologies (WGTYP).

11. This project was undertaken in the FATF WGTYP. The co-chairs of the project were the International Monetary Fund (IMF), United Kingdom (UK), United States (US) and World Bank. Source material for the project included a review of the relevant literature, consultation with Dr. Peter Reuter[8] and Dr. Matthew Hitchcock Fleming,[9] survey responses from FATF members describing jurisdictional risk assessment methodologies and terminology, contributions from the core project group[10] and related discussions in Bangkok, Thailand at the November 2007 FATF Typologies Experts' Meeting.

12. The first section of the report describes what a national ML/TF risk assessment is and what a risk assessment project entails. While the risks and the priorities may vary from one country to another, much of the information gathering and even the assessment process are built into the FATF Recommendations.[11] The 40+9 Recommendations and the role of financial institutions, regulatory and supervisory authorities, financial intelligence units, and law enforcement are mapped to the assessment process in this first section.

[6] Ibid.

[7] For more on why to conduct a national money laundering/terrorist financing risk assessment, refer to FATF (2007a).

[8] Dr. Reuter is a professor in the School of Public Policy and the Department of Criminology at the University of Maryland in the United States.

[9] Dr. Fleming is currently serving as a Highly Qualified Expert with the US Department of Defense; he was a consultant on AML/CFT matters with the IMF at the time of drafting of this report. He has also held positions with the IMF, World Bank, United Nations, and with University College London's Jill Dando Institute of Crime Science.

[10] In addition to the IMF, UK, US and World Bank, the core project team included Australia, Belgium, and the Netherlands.

[11] See *The FATF 40+9 Recommendations* .

13. The second section of the report presents examples of jurisdictional risk assessments covering money laundering and/or terrorist financing. The methodology and output of these efforts varies, but together they illustrate the many approaches that can be taken to understand how terrorists and criminals move money within a jurisdiction.

14. The third section of the report addresses the environment in which a national ML/TF risk assessment is produced, describing the process and resources needed. A national risk assessment may be a collection of single agency efforts or a coordinated multi-agency project. Either approach is resource-intensive requiring information and cooperation from competent authorities.

15. The fourth section of the report provides guidance to relevant information sources and analytical methods that may provide information helpful to understanding the scope of money laundering and/or terrorist financing beyond what can be identified through law enforcement investigations and financial institution currency and transaction reporting.

16. The report concludes with suggestions for further study, focusing on FATF Recommendations 31 and 32. These Recommendations address the need for relevant data and cooperation among competent authorities, which are the two fundamental building blocks of a national ML/TF risk assessment. Although authorities may prefer to work independently on mission-specific ML/TF risk assessments, this approach could suffer from a lack of scope and relevant information unless opportunities exist for the relevant authorities to reinforce one another's risk analysis and resulting AML/CFT strategy.

17. Appendix 1 is a summary of the responses received to the project survey issued through the FATF WGTYP. Appendix 2 describes a model that can be used to help evaluate the effectiveness of law enforcement. Appendix 3 provides a framework to go beyond known data to estimate the full scope of money laundering in a jurisdiction.

I. WHAT IS A RISK ASSESSMENT?

18. Many industries conduct risk assessments. Depending on the circumstances, a risk assessment can be retrospective or prospective, quantitative or qualitative, or some combination. A quantitative risk assessment, using valid data, can be more objective and more useful over time than a qualitative risk assessment developed from assumptions and random case studies.

19. Retrospective risk assessments have the benefit of drawing on data from past events to help anticipate future problems.[12] Although the past is not always a reliable indicator of the future, consistent patterns can emerge in data and crime data is no exception.

20. Prospective risk assessments attempt to see into the future without the benefit of historical data.[13] The risk assessment process when little or no data is available involves using whatever information is known to anticipate real or potential outcomes. This approach relies primarily on qualitative rather than quantitative indicators.

21. The best risk assessment methodology uses a combination of approaches in order to capture all that is known and as much as possible about what is not known.

22. There are likely to be illicit financing methods being used that have not been detected by financial institutions or law enforcement, and so will not show up in the data gathered from criminal investigations or financial institution currency or transaction reporting. And there may be other illicit financing options that even the criminals have not yet discovered. In the absence of data or case studies identifying these methods, financial institutions and competent authorities must rely on creative intuition and a careful analysis of potential systemic weaknesses.

Conducting a National ML/TF Risk Assessment

23. A national ML/TF risk assessment is an organised and systematic effort to identify and evaluate the sources and methods of money laundering and terrorist financing and weakness in the AML/CFT systems and other vulnerabilities that have an impact, either direct or indirect, on the country conducting the assessment. Such an assessment may involve multiple public sector offices working together with or without the private sector, or it may involve one or more individual agencies working independently to assess specific aspects of the country’s ML/TF situation.

24. An assessment effort that is organised and systematic is one that has a well-defined process and purpose with clearly stated goals. Also important is that sufficient resources are available, including information, to achieve the stated goals.

[12] Life insurance companies study, among other things, the circumstances involved in the deaths of policyholders to look for indicators of premature death that will help in pricing future policies. Auto insurers study accidents, particularly those involving their policyholders, in order to identify indicators of poor driving habits. Financial analysts study historic pricing patterns for financial stocks and bonds. Price fluctuation is perceived as “risk” in financial markets. Doctors and pharmaceutical manufacturers test experimental treatments on small groups of patients in order to anticipate positive and potentially negative outcomes in the general population.

[13] This kind of assessment is common in industries in which a single accident or malfunction can have horrific consequences, limiting potential testing (*e.g.* aircraft design, nuclear power plant operations, and disaster preparedness).

25. Although depth of coverage may differ, a national ML/TF risk assessment is a process that typically presents information on:

- The nature and scale of ML/TF and related predicate crimes (*i.e.* the *threat*).
- Weaknesses in AML/CFT systems and controls and other features of a jurisdiction that make it attractive to money launderers and terrorist financiers (*i.e.* the *vulnerability*).

26. Assessing the nature and scale of ML/TF and related predicate crimes involves identifying and quantifying the predicate crimes and methods supporting money laundering and terrorist financing, using law enforcement investigations, prosecutions, and convictions, as well as financial institution currency and transaction reporting, and other relevant data.

27. Assessing weakness in the AML/CFT systems and controls involves determining whether appropriate laws are in place to block or deter certain illicit financing activity. Where adequate laws are in place yet data shows that illicit activity is occurring at an unacceptable rate the effectiveness of law enforcement has to be evaluated, as well as the potential impact of corruption.

28. The output of a national ML/TF risk assessment is generally a public document, although in some jurisdictions, a restricted version may also be produced which may elaborate on specific criminal (and, potentially, national security) intelligence.

29. The national ML/TF risk assessment should be an input to a national strategy, as part of the country's overall AML/CFT risk management process.[14]

30. The extent to which an assessment can identify and evaluate ML/TF threats depends on the information available. At a minimum, identifying the common predicate crimes that generate illicit proceeds and the subsequent money laundering methods used should be a routine function of domestic law enforcement. Going beyond identifying to quantifying and evaluating the money laundering/terrorist financing situation requires data from investigations, prosecutions, and convictions; financial institution currency and transaction reporting; and relevant indicators of potential criminal activity.

31. Although evaluating the scale and scope of ML/TF is valuable, just identifying all of the relevant methods of illegal financial activity is often challenging. The risk assessment process will require that judgments be made about the information available, including what information to use, how to use it, and even how to interpret it. For example, determining what constitutes "domestic" money laundering or terrorist financing can itself be a challenging question. The globalisation of trade, increasing use of the Internet, and introduction of new payment methods has made it difficult to determine where crimes are committed or where the associated transactions take place.

32. Regardless of whether a national ML/TF risk assessment is quantitative or qualitative, retrospective or prospective, the inputs to the risk assessment process – both objective and subjective sources of information – should be clearly identified along with any assumptions or interpretations.

The FATF Recommendations and the Risk Assessment Process

33. Whether a national ML/TF risk assessment is drawn from risk assessments conducted by individual public sector agencies working independently or is coordinated as a single effort with broad participation, the private sector, regulatory and supervisory authorities, FIU, and law enforcement

[14] The strategy should address the vulnerabilities identified in the risk assessment (*e.g.* implement or amend laws as appropriate, study identified problems in greater detail as necessary, reallocate resources to cover law enforcement inadequacies, and/or focus on personnel or agencies suspected of creating vulnerabilities through corruption).

community each competent authority involved in AML/CFT has a unique vantage point to make a contribution to the ML/TF risk assessment process.

34. Regardless of which offices of the national government collaborate to produce a national ML/TF risk assessment, the process should involve public and private sector information and expertise:

> *"Public authorities, whether law enforcement agencies, regulators or other bodies, have privileged access to information that may assist financial institutions to reach informed judgments when pursuing a risk-based approach to counter money laundering and terrorist financing. Likewise, financial institutions routinely transact with a great number of customers on a daily basis, and are able to understand their clients' businesses reasonably well. It is desirable that public and private bodies work collaboratively to identify what information is valuable to help combat money laundering and terrorist financing, and to develop means by which this information might be shared in a timely and effective manner."*[15]

35. This public-private dialogue and the resulting risk assessment should inform both the public and private sectors in their risk-based procedures in order to create and maintain a common vocabulary and set of shared experiences and expectations.

36. The AML/CFT procedures addressed in the FATF Recommendations that apply to the private sector and competent authorities can yield relevant data and guidance on which to base a national ML/TF risk assessment (see Table 1).

37. The Terrorist Financing report observes that: "Through the development of internationally recognised AML and CFT standards, financial institutions and other designated non-financial entities have taken steps to know their customers and keep records. The value of financial information in counter-terrorism investigations has increased dramatically in recent years. [16]

[15] FATF (2007a).

[16] FATF (2008).

Table 1. Mapping the FATF Recommendations to the ML/TF risk assessment process

Private/ Public Sectors	FATF Recommendations	Support for Risk Assessment
Financial Institutions	Policy/procedures for customer due diligence (R.5)	Helps identify high-risk customers Helps identify high-risk transactions
	Policy/procedures for enhanced due diligence for politically exposed persons (R.6)	
	Policy/procedures for non-face to face business relationships (R.8)	
	Policy/procedures for anti-money laundering & counter terrorist financing programs (R.15)	
	Policy/procedures for countries that do not apply or insufficiently apply the FATF Recommendations (R.21)	
	Identify unusual and report suspicious transactions (R. 11 & 13)	
	Consider identifying and reporting large currency transactions (R.19)	
Regulatory/ Supervisory Agencies	Establish AML/CFT guidelines for financial institution policies and procedures and provide feedback (R.25)	Suggests criteria for identifying high-risk customers and transactions and the adequacy of compliance by financial institutions
	Monitor and ensure AML/CFT compliance (R.29)	
	Coordinate and cooperate on AML/CFT with policy makers, the FIU, and law enforcement (R.31)	Coordinate on national AML/CFT strategy
	Maintain comprehensive statistics on supervised institutions and supervisory efforts (R.32)	Develop statistics for retrospective risk assessment
Financial Intelligence Unit	Coordinate and cooperate on AML/CFT with policy makers, supervisory authorities, and law enforcement (R.31)	Coordinate on national AML/CFT strategy
	Maintain comprehensive statistics on currency and transaction reports filed by financial institutions (R.32)	Develop statistics for retrospective risk assessment
Law Enforcement Authorities	Coordinate and cooperate on AML/CFT with policy makers, supervisory authorities, and (R.31)	Coordinate on national AML/CFT strategy
	Maintain comprehensive statistics on AML/CFT investigations, prosecutions and convictions; asset seizures/forfeitures; and on international requests for co-operation. (R.32)	Develop statistics for retrospective risk assessment

II. EXAMPLES OF NATIONAL ML AND/OR TF ASSESSMENTS

38. A relatively small number of countries have conducted a national assessment of money laundering and/or terrorist financing. These efforts use different approaches and often different sources of information, but each offers instructive insight into the national risk assessment process.

39. The models that were followed include a multi-agency national assessment; a national organised crime threat assessment covering money laundering; a "one-off" academic research project on the domestic money laundering situation; and a single-agency money laundering threat assessment. Many countries as well as the FATF have examined specific financial sectors or particular money laundering methods through typologies studies.

40. Drawing mainly upon the survey results but also on follow-up interviews and the literature review, this chapter sets out various examples of national assessments:

Australia

41. In 2004 Australia undertook its first attempt at a national assessment of money laundering threats through a report commissioned by the Criminology Research Council (a joint Australian, State and Territory Government initiative to research criminological issues in Australia). This research report attempted to explore the range of new types of information developed in the last decade by the establishment of national and international agencies and networks responsible for monitoring money laundering, and to establish the extent of money laundering in and through Australia in 2005, and how it had changed since1995. Specifically, the report aimed to:

- Examine and update a previous 1995 report on the *Estimates of the Extent of Money Laundering in and through Australia* (the 1995 Walker report).
- Extend the analysis of the extent of money laundering to include assessments of the linkages of crime and money laundering in the Asia Pacific region and an examination of the linkages of money laundering to terrorism in the region.

42. In addition, the Report aimed to determine the orders of magnitudes of the component parts of money laundering in and through Australia, to determine what level of effort is appropriate to counter money laundering, and what key directions those efforts should take. The purposes of understanding and trying to quantify money laundering were three-fold:

- To assist in deterring criminals by attacking their enjoyment of the proceeds of crime.
- To assist in preventing acts of terrorism by attacking their sources of funding.
- To assist in determining the actual impacts of money laundering on society and the financial system, so that counter-measures are proportionate to the actual threat.

43. The underlying methodology of the report was to apply the principle of triangulation, which in effect requires the mixing of qualitative and quantitative approaches. The author's triangulation approach used a combination of methods to explore research questions and the problems related to the data gathered. Data was collected in a variety of ways, from various perspectives, and from different reference points. This enabled the author to compare and contrast the findings, corroborate the understandings and interpret the data. Specifically the methodology used, but was not limited to:

- A review of the relevant literature post 1995 including responses to the 1995 Walker report.
- Assessment of relevant Australian, State and Territory Government Annual Reports and other official statistics.
- A survey of Law Enforcement agencies, researchers and criminologists as well as Financial Intelligence Units in Australia and overseas, followed by interviews with selected individuals.
- Consideration of other research and examination of AUSTRAC data.

44. The following offices participated in the report:

- Australian law enforcement agencies.
- AUSTRAC's counterpart FIUs in other countries.
- Researchers/criminologists in Australia.
- Researchers/criminologists overseas.

45. The judgments made were primarily qualitative in nature based on academic research and review.

Belgium

46. The Belgian FIU, la *Cellule de Traitement des Informations Financières* (CTIF-CFI), undertakes typological analysis of its operational files to describe techniques used by criminals for laundering money of illegal origin. By identifying the typological characteristics in the files forwarded to the judicial authorities, CTIF-CFI aims to enhance the detection of suspicious transactions by the disclosing institutions and persons, thus preventing the use of the financial system for money laundering purposes.

47. The typological study covers a one-year period and refers to the files forwarded to the judicial authorities during this period. Developments in the methods to launder criminal profits become clear by means of *general trends* that can be deduced from the evolution compared to previous years. Apart from identifying general trends, the study also takes into account *specific trends* based on the analysis of the files reported during the year. These files specifically highlight certain aspects of money laundering characteristics for the files reported during the year. These trends generally reveal great diversity of disclosing parties, money laundering, and terrorism financing methods and techniques, and illustrate the importance of cooperation among all relevant parties, both at the national and international level.

48. The results of such studies are published in CTIF-CFI's annual report and are available on CTIF-CFI's website (www.ctif-cfi.be). Moreover, the results of such studies are also presented to the private sector during information sessions.

49. Only CTIF-CFI participates in its own threat assessments but external official sources of information are consulted to find out if they confirm the findings of the common characteristics. These external official sources include reports published by international organisations (UN, FATF, Egmont Group, EU, etc.), by national public authorities (senate, parliamentary investigation committees, police services, state security services, etc) or by the supervisory or regulatory authorities (banking, finance and insurance commission, etc).

50. Apart from identifying trends based on the analysis of the files reported during the year, CTIF-CFI also performs typological studies on thematic issues. Examples have included recently, typologies concerning financial transactions, specific phenomena, and predicate offences or reporting entities. Those studies are also available on CTIF-CFI's website and are intended to enhance the detection of suspicious transactions by the disclosing parties.

Canada

51. Canada is in the first stage of developing a framework for a National Threat Assessment. Canada is grappling with the distinction between a quantitative data-based threat assessment and the collection of strategic intelligence already undertaken by law enforcement in partnership with other government departments (outlined below).

52. Canada's Mutual Evaluation Report identified the need to introduce a formal process for assessing the level of risk inherent in a particular financial product or sector. It is envisioned that this risk assessment will feed into Canada's overall Threat Assessment.

53. The Canadian Intelligence Working Group (IWG) is led by the Royal Canadian Mounted Police (RCMP) and includes representatives from the Department of Finance, the Canada Revenue Agency (CRA) and Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The focus of the IWG is the gathering, analysis and dissemination of strategic intelligence regarding laundering and organised crime activities. This intelligence is shared with law enforcement agencies and other domestic and international partners.

54. The IWG undertakes both tactical and strategic projects aimed at identifying money laundering typologies and new trends in financial products that could be used by different organised crime groups to launder their assets in Canada and abroad. Currently the IWG is working on three major tactical projects focusing on outlaw motorcycle gangs, East European organised crime and Asian organised crime groups.

55. In addition, several intelligence reports are produced throughout the year on specific strategic subjects and specific tactical intelligence by both the RCMP and FINTRAC. Other reports are produced at the request of international partners through the International Liaison Officers Program or through the Department of Finance on behalf of the FATF and the Asia Pacific Group on Money Laundering. Not all of these reports are publicly available.

56. The IWG is in the initial phases of three new strategic projects concerning white label ATMs, e-currencies/cross border currencies and stored value cards. The resulting analysis and conclusions from these tactical and strategic projects may be used in the preparation of a threat assessment report that is scheduled for the fall of 2008.

57. To complement the interdepartmental working group a Public/Private Sector Advisory Committee has been created. It is anticipated that the private sector will contribute to the National Threat Assessment.

Japan

58. The Japan National Police Authority (NPA) produces a national assessment report focusing on the national organised crime situation, including an analysis of money laundering. The money laundering assessment is drawn from an examination of completed cases, identifying new methods, typologies and relevant statistics. The NPA also gathers statistics on the number of suspicious transaction reports annually and cases involving money laundering. It provides relevant institutions with these results and as well as making some information public.

Macao, China

59. The Financial Intelligence Office was established in 2006 to receive, analyse, and disseminate information from suspicious transaction reports. The Office also takes up the coordination role of the Government Working Group. The main information it receives comes from suspicious transaction reports (STRs) and statistics on investigations, prosecutions, and convictions that are provided by the

Judiciary, Police and Public Prosecution Office. The Government of Macao is considering carrying out a national threat assessment through the Financial Intelligence Office.

60. The quantitative methods will include statistical analysis of the STRs received and cases under prosecution. The data should cover the type of predicate offence, amount of money laundered, currencies involved, source and destination of funds, amount of assets being seized and confiscated, etc. Qualitative methods will cover analysis on trends and development of money laundering methods used and problems encountered in unsuccessful prosecution cases or any problems on supervisory issues.

Netherlands

61. Following a similar approach to the model used by the Australian Government, in 2005, Dr. Brigitte Unger of the Utrecht School of Economics, conducted a study titled "The Amounts and Effects of Money Laundering."[17] The study was assigned and funded by the Ministry of Finance. Its objective was to obtain better information on the amount, flows and effects of money laundering, using a macroeconomic approach. The results were used as input for further policy formulation.

62. The study by Unger relied on two approaches. A quantitative method was used to estimate the amount, flows, and effects of money laundering. The Walker (1995) model was replicated and re-estimated by using crime rates and expected proceedings from crimes. This results in a national demand for money laundering. In order to gain insight to the international dimension of money laundering, scores were calculated for countries based on the estimated flow of illicit funds. A country with a relatively high score on the attractiveness index for money laundering will face larger inflows of the world's 'dirty' money. Also calculated was how much of the estimated total proceeds from Dutch criminal flows abroad and how much stays in the Dutch economy.

63. In addition, an extensive literature search on definitions, typologies and growth effects was performed for both the Dutch, and the global economy. There is some discussion on related areas of study, for example on the spending behaviour of criminals and the effect of money laundering on foreign aid. The author also identifies typical Dutch forms of money laundering. The findings made were mainly qualitative judgments but sometimes supported by quantitative data.

64. The research by Professor Unger was conducted by the Utrecht School of Economics, in conjunction with the Australian National University. A multi-agency approach was followed including consultations with: the Dutch Central Bank, Ministries of Finance and of Justice and the Netherlands Financial Intelligence Unit, Economic Investigation Service.

65. In addition to the project on the amount and the effects of money laundering, every four years the National Police Services Agency (KLPD) publishes a National Threat Overview that focuses on developments in the field of serious and organised crime. This study also includes a section about money laundering and is primarily based on data-analysis and expert interviews.

66. The Research and Documentation Centre (WODC) of the Ministry of Justice has also constructed an Organised Crime Monitor. This instrument helps policy-makers to identify the nature, size and impact of organised crime in the Netherlands and is used as a basis for other studies in this field.

Poland

67. The Polish annual national money laundering threat assessment aims to identify new methods of money laundering and to indicate the levels of the identified methods. This is a multi-agency assessment. It relies on criminal typology information derived from money laundering cases held by

[17] Unger (2006).

the Polish FIU, as well as reports from the FIU to the offices of the Public Prosecutor identifying cases with a well-founded suspicion of money laundering; reports from the Ministry of Justice; and reports from the Ministry of Interior and from the National Police Headquarters.

68. The results of the Polish national money laundering threat assessment are presented in annual reports and periodically in manuals provided to financial institutions and cooperating units, however this information is not released to the public.

Spain

69. The Centre of Intelligence Against Organised Crime (CICO), created in 2006, collects and integrates all information related to organised crime as necessary for developing the general strategy against these groups. The CICO, under the Ministry of Interior, is aimed to establish the coordination criteria between the law enforcement units involved in the AML field. It will prepare an annual report on the assessment of the threat of money laundering, and the effectiveness of the AML measures, as well as statistics related to money laundering schemes, infringements, and investigations conducted.

70. The Commission for the Prevention of Money Laundering and Monetary Offences (CPBC) has drafted a list of risk transactions that identify money laundering vulnerabilities. This listing of vulnerabilities is known as COR, that is, examples of high-risk transactions. The CPBC has published COR regarding to the following sectors: stock exchange, insurance, money remitters, professionals, real estate and banking institutions. Relevant institutions from the private sector, such as: the Spanish Private Banking Association, the Spanish Confederation of Savings Banks, as well as individual professional bodies including Associations of Real Estate companies, the Accounting and Auditing Institute, the General Council of Law and the General Council of Notaries, have participated in the elaboration of the COR.

71. Such lists of transactions are aimed to help the obliged entities to fulfil the requirements included in the AML regulation and to identify possible transactions linked to money laundering or terrorist financing activities, as well as high risk customers, special products and services and high risk business activities. The Annual Report, available on the SEPBLAC website[18], includes a chapter containing a description of the most relevant case studies analysed during the year.

72. Based on the catalogues, the obliged entities have prepared specific risk checklists to be circulated among all employees, which are regularly reviewed and updated depending on how circumstances develop and how threats evolve.

73. The CBPC, which includes all relevant agencies with AML/CFT responsibilities, devised and approved the AML National Strategy in 2002. It consists of 3 main objectives, 12 strategies and 21 actions, assigned to each of the members of the Commission. The first objective of this strategy has been to give support to reporting entities in the implementation and improvement of laundering prevention measures. This objective is to be pursued through the following strategies:

- Establishing a regular discussion with reporting parties to analyse and exchange experiences regarding suspicious transactions and facilitate pre-emptive measures regarding risk sectors, practices and geographical areas (national and international).
- Strengthening the reporting parties’ inspection programme.
- Reviewing certain prevention measures that are part of the routine inspection duties of supervisory agencies.
- Promoting training within reporting parties.

[18] SEPBLAC is the name of the Spanish financial intelligence unit: www.sepblac.es.

- Engaging additional sectors and activities (private banking; internet banking; use of correspondents; group subsidiaries) in the fight against laundering.

United Kingdom

74. The United Kingdom Threat Assessment (UKTA) produced by the Serious Organised Crime Agency (SOCA) describes and assesses the threats posed to the UK by serious organised criminals and considers how those threats may develop in future. There is a section dedicated to criminal finances and profits, and money laundering is also covered as a crosscutting theme.

75. A protectively marked version of the UKTA is produced to inform both UK law enforcement priorities for tackling serious organised crime and other relevant initiatives, such as changes in legislation, regulation or policy. The Not Protectively Marked version is aimed at increasing public awareness, thereby helping individuals to protect themselves from becoming the victims of serious organised crime.[19] A SOCA representative[20] estimated that the public version of the UKTA comprised approximately 40 per cent of the text used in the classified version.

76. The UKTA is a collaborative effort. It draws on information from a wide range of sources, both in the UK and abroad. In regard to money laundering issues, the principal sources are operational reporting both from the UK and overseas, Government Departments, STRs, databases and public information. The judgments are mainly qualitative in nature though some specific quantitative measurements are used.

77. Building upon the UK Threat Assessment and the National Intelligence Requirement (NIR)[21], the Organised Crime Control Strategy sets out how UK agencies, working with partners, plan to tackle organised crime. The 2007 AML/CTF Strategy titled “The Financial Challenge to Crime and Terrorism”[22] drew upon the findings of the UK Threat Assessment and the Control Strategy. This document assessed progress against key objectives and set out the AML/CTF Strategy for the next three to five years. Going forward, it sets out “building knowledge” of money laundering and terrorist financing as a key future objective.

78. The UK FIU (SOCA) also undertakes a number of typologies. Recent subjects have included a typology on the money laundering threat posed to the UK by politically exposed persons and also money laundering through casinos. The typologies drew upon operational intelligence, on-site visits to banks or casinos, database information, consultations with government departments and industry, as well as an examination of indicators in an attempt to identify the economic impact to the UK. The typology was not made publicly available but was shared with industry through a vetted group.

79. In July 2005, the Chancellor and the Home Secretary asked Sir Stephen Lander to review how the UK SARs regime could best be managed under SOCA. In the report known as the “SARs Review”[23], Sir Stephen makes 24 recommendations to improve the system, primarily focusing on the role of SOCA as the regime’s FIU. These recommendations include improving the underpinning IT, improving the training and guidance provided by the FIU, and facilitating better dialogue between the regime’s participants.

[19] Serious Organised Crime Agency (SOCA) (2006).

[20] Interview conducted with Principal Officer, SOCA, 5 February 2008.

[21] The NIR, also produced by SOCA, acts as a guide to agencies that hold or collect information and intelligence of relevance to serious organised crime, identifying the gaps in knowledge and priorities for filling them.

[22] HM Treasury (2007).

[23] SOCA (2006).

United States

80. In 2005, the United States initiated its first multi agency money laundering threat assessment. Quantitative inputs included prosecution data from federal law enforcement agencies and suspicious transaction reporting via the FIU. Qualitative inputs came from law enforcement and regulatory authority case studies with private sector reporting.

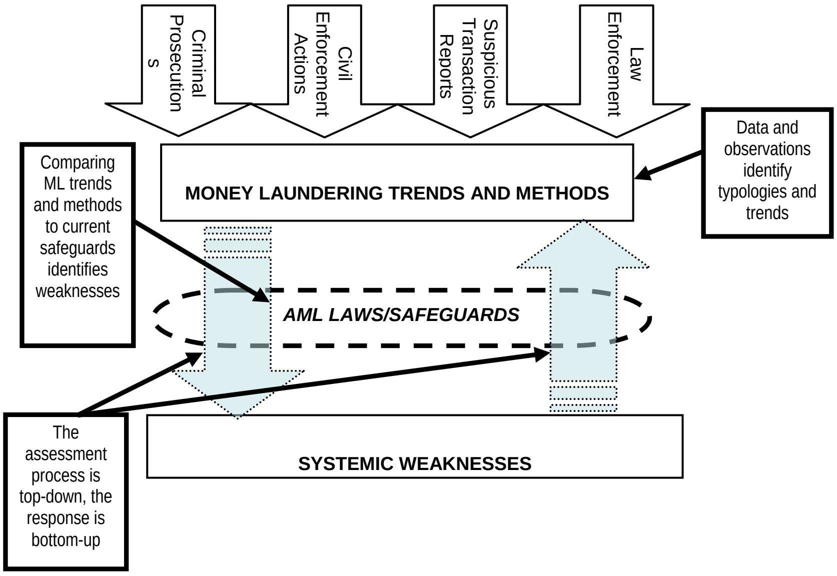
81. The 2005 U.S. Money Laundering Threat Assessment[24] was divided into the following sections: banking, money services businesses (*i.e.* money transmitters, check cashers, currency exchangers, money orders, and stored value cards); online payment systems; informal value transfer systems; bulk cash smuggling; trade-based money laundering; insurance companies; shell companies and trusts; and casinos.

82. The project team made assumptions and observations about vulnerable sectors using the available information, considered whether adequate safeguards were in place to address the identified vulnerabilities, and made a subjective determination about the residual threat.

83. This was a multi-agency process including offices/agencies under the U.S. Departments of Homeland Security, Justice, and Treasury. Also participating was the Board of Governors of the Federal Reserve System and the United States Postal Inspection Service.

84. The available information was synthesised to form a qualitative assessment, which included, to the extent possible, the relative effectiveness of AML safeguards. In some cases, data was available to support subjective judgments regarding effectiveness (see Figure 1). Otherwise, the determinations were the result of broad intergovernmental discussion and analysis.

Figure 1. Flow chart depicting U.S. money laundering assessment and strategy formation process


Criminal Prosecutions
Civil Enforcement Actions
Suspicious Transaction Reports
Law Enforcement
Data and observations identify typologies and trends
Comparing ML trends and methods to current safeguards identifies weaknesses
MONEY LAUNDERING TRENDS AND METHODS
AML LAWS/SAFEGUARDS
The assessment process is top-down, the response is bottom-up
SYSTEMIC WEAKNESSES

Europol

85. Europol produces an annual Organised Crime Threat Assessment (OCTA) [25] for the EU. The OCTA is a core product of the intelligence-led policing approach. It fits in firmly with The Hague Program objectives and is complemented by the development of the European Intelligence Model. As well as a number of countries law enforcement agencies, many European organisations and institutions

[24] Money Laundering Threat Assessment Working Group (2005).

[25] EUROPOL (2007),

were involved in the drafting including the European Central Bank, Eurojust, OLAF, Frontext and OLAF. Furthermore, a number of representatives from academia and the Private Sector were involved.

86. In regard to money laundering, this is covered in a chapter titled “exploitation of the financial sector”. The document was endorsed by the European Council at their meeting of 6 June 2006.

Interpol

87. Interpol has also produced studies into money laundering trends. Two recent examples include “Alternative remittance systems distinguishing sub-systems of ethnic money laundering in INTERPOL member countries on the Asian continent” [26] and “The hawala alternative remittance system and its role in money laundering.” [27]

[26] Carrol, L. (2007).

[27] Jost, Patrick and Harjit Sandu (2000).

III. ISSUES TO CONSIDER WHEN CONDUCTING A NATIONAL ML/TF RISK ASSESSMENT

Meeting the Needs of the Customer

88. The customers of the national ML/TF risk assessment can include government departments, the private sector, non-governmental organisations, and the public. The objectives of the assessment will vary according to the customer. For example, the national assessment could be a tool for government officials to consider policy or strategy formulation. It may be that the objective of the assessment is simply to describe the current money laundering situation. In other cases though there may be an expectation that there is some analysis of the effectiveness of the counter-measures. The expectations will have an impact on the scale of ambition and the consequent resource allocation that will be required.

89. An objective of the assessment could be to provide information for the public and to enhance the general understanding of government initiatives. One challenge to overcome is that some information within the national assessment may be derived from classified sources. As such, some countries produce a non-classified version for the public. However, the sensitivity of some of the intelligence sources may be a barrier. Some survey respondents addressed this challenge by establishing a private sector group with which they can communicate the key findings from the assessment. In the UK a "vetted" group of private sector representatives has been established to receive more sensitive information.

Resources and the Assessment Process

90. Resource considerations for a national ML/TF assessment include personnel, time, and access to information. Countries acknowledge the work to collect and examine information for a national ML/TF risk assessment can be time consuming. Meetings, interviews, data corroboration, and analysis can be a lengthy process, particularly if various offices of competent authorities disagree on the threats and vulnerabilities.

91. When several government agencies work together to produce a national assessment a central coordinating body is useful to manage the gathering and analysis of information. Often this is situated in the lead government ministry for AML and/or CFT, though the coordinating office may also be situated in the FIU or an inter-departmental working group may be preferred. This body would be tasked with managing the information collection process, analysis, and reporting timeline and producing the final assessment document.

92. A number of countries undertaking a multi-agency assessment felt that a clear production plan was useful. The various steps, milestones and participants within this will vary according to the national circumstances and the scale of ambition of the assessment.

93. The countries that currently undertake multi-agency assessments organised the information according to sectors. In the organised crime assessment models, chapters are often organised according to particular crime methods or predicate offences.

94. In order to extract best value from the available resources intelligence/information gathering efforts should be prioritised in key areas. An "intelligence requirements" or "contract" can be developed which broadly sets out the key areas in which information is required. This can, if

necessary, be refined into a more detailed information collection plan; this is often seen in the organised crime assessment model where high level intelligence requirements may be initially set out which are then refined according to the specific type of criminal behaviour being examined.

95. The requirements document should evolve year on year, in response to the findings made in assessments. For example, an annual assessment may conclude that there is some evidence of certain money laundering methods or trends but that there is insufficient information to reach definitive conclusions. Therefore there is need for more intense information gathering in this area in the following year, so that more accurate judgments can be reached.

Interagency Cooperation

96. A multi-agency national assessment will comprise many different cooperating participants from various government ministries, including law enforcement and intelligence agencies. In some models non-governmental bodies may also be involved, such as trade associations or other private sector representatives. In any multiagency setting, there can be competing or conflicting objectives between the various actors.

97. One challenge that can arise is an unwillingness to accept unwelcome findings. Agencies concerned that financial industries or sectors under their responsibility will be seen as vulnerable to money laundering or terrorist financing may be unwilling to share information or endorse the risk assessment team's conclusions.

98. Establishing clear terms of reference at the beginning of the process, defining the roles and responsibilities of participants, and ensuring that senior officials are overseeing the process may help to avoid difficult situations. The terms of reference can provide a useful reference point throughout the drafting process to ensure the assessment is "fit for purpose" and can provide a checkpoint to examine the final product when delivered.

99. Regular review and discussions with key participants are useful for ensuring that all relevant agencies are fully involved in the process. For example, the production process for the UK Organised Crime Threat Assessment includes two specific sessions for each of the chapters so that key customers attend to bolster the intelligence and reach a consensus, while analysts attend to provide the analytical questioning and framework.

Data Availability and Quality

100. In order for a national ML/TF risk assessment to represent the most accurate findings, analytical judgments within the assessment should be based on objective information wherever possible. This information may be derived from various sources (both qualitative and quantitative). The availability and quality of information will vary considerably amongst jurisdictions. Countries with limited data on criminal investigations or financial transactions will still be able to conduct a risk assessment but may need to rely more on expert judgment and international data sources. Moreover, a national assessment may conclude that one of the significant systemic vulnerabilities is the presence of information gaps that need to be filled.

Developing an Ongoing Assessment Process

101. Money laundering and terrorist financing methods are not static phenomena; they evolve and respond to law enforcement actions, legal changes, new technologies, and national societal circumstances. As such, it may be desirable to monitor the development of ML/TF threats over time. This may require referring back to the judgments made in previous assessments and examination of earlier statistics in order to determine whether there are noticeable changes.

102. Maintaining a consistent approach to the assessment process, using the same quantitative and qualitative indicators, is important to compare findings over time. However, the desire to compare results year to year should not override the need to fix methodological flaws or add new data sources as appropriate.

103. A number of respondents to the project survey indicated they compare the conclusions in their national assessment to results reported by other countries and multinational organisations. Because of differing methodologies, including different quantitative and qualitative data and analytical approaches, risk assessments may not be directly comparable without making adjustments.

IV. SOURCES OF DATA FOR A NATIONAL ML/TF RISK ASSESSMENT

Determining the Threat

104. Central to the understanding of a jurisdiction's ML/TF risk is an understanding of the *threat* it faces. The level of threat a jurisdiction faces is affected in part by its vulnerability to money laundering and/or terrorist financing. A jurisdiction with very weak systems and controls – a vulnerable jurisdiction – may find itself with more predicate crime than otherwise would be the case, and may also be an effective haven for terrorist financing.

105. Assessing the TF threat is challenging due to the variety of ways terrorists raise, move, and use money. Terrorists use legitimate and illegitimate sources of income as well as state sponsors:[28]

- *Legitimate Sources*: Terrorist organisations receive considerable support and funding from and through legitimate sources including charities, businesses, and in many cases through self-funding from employment, savings, and social welfare payments – methods that would not otherwise raise concerns because they appear legitimate. Case studies highlight the value of intelligence in determining whether seemingly legitimate activity is being used to fund terrorism.
- *Criminal Activity*: Terrorist groups are increasingly turning to alternative sources of financing, including criminal activities such as arms trafficking, money laundering, kidnap-for-ransom, extortion, racketeering, and drug trafficking. Terrorist use of criminal activity to raise funds ranges from low-level fraud to serious organised crime.
- *State Sponsors*: Safe havens, failed states and state sponsors continue to represent crucial sources of support for terrorist organisations today. Safe havens and wider cases of weak jurisdictional control, state tolerance or support of terrorist organisations are also important in how terrorists move and use finance, in addition to their role in raising terrorist fund.

106. The money laundering threat refers to the nature and scale of money laundering and predicate crimes, and can be thought of as the demand for money laundering.[29]

107. Predicates of laundering differ by jurisdiction, but generally should include, at the very least, the 20 crime categories set forth in the glossary of the 40 FATF Recommendations. To these predicate offenses could be added money laundering, which also generates illicit proceeds for the specialist launderer, as well as illegal gambling, illegal prostitution, tax evasion, and other crimes committed for financial gain. Some crime types will clearly command a higher demand for laundering than others.

108. The challenge to understanding the money laundering threat lies with the ability to measure the nature and extent of diverse predicate crimes and their resulting proceeds in order to reflect underlying crime trends and patterns. Attempting this requires an understanding of the measurement of crime and the limitations of crime data.

[28] FATF (2008).

[29] For more on demand for money laundering see Reuter and Truman (2004).

Measuring Crime

109. Crime is measured through various public and private sector statistics. The most traditional source of information on crime is official administrative data captured by one or more jurisdictional bodies.[30] Most common data points relate to the volume or incidence of recorded crime, arrests, prosecutions, and convictions.[31]

110. The most important limitation to official crime statistics is that they only represent a portion of the overall population of crime. There is an unknowable population of total crimes carried out over a period of time. Even some predatory crimes fail to be reported; so known crimes will only represent a subset of total crimes.[32]

111. A subset of known crimes will be reported crimes. A subset of reported crimes will be recorded crimes and a subset of those will lead to an investigation. Some investigations will lead to an arrest, and some arrestees will eventually be prosecuted. Of these individuals a subset will be convicted. The point is that there is attrition in the process and in the data (see Figure 2).

112. Even for known crimes, different jurisdictions may employ different methods for counting crime and, indeed, the same jurisdiction may change its counting method over time, with implications for comparability. When a crime incident comprises multiple crimes, such as a murder and a robbery, the most popular approach embodies counting the most serious crime. In this regard, however, criminal statistics will fail to capture the true nature and extent of crime generally; as such, several jurisdictions are moving to recording crime on a per incident basis, such that the entire series of connected crimes will be recorded in a relational sense.

113. Official crime data must be interpreted with care. High rates of reported or recorded crime may be the result of an active law enforcement community rather than an indication of high rates of crime relative to a comparable jurisdiction. When using prosecution and conviction data, as opposed to crime reports, it is important to remember that certain types of crime, particularly money laundering, are charged less frequently in certain jurisdictions or may be plea-bargained away, [33] even though the crime has occurred, and so the official data may not be truly indicative of the actual underlying trends.

114. Another shortcoming with frequently collected official crime data is that these statistics often focus on violent crime, not the profit-driven crimes that comprise most predicates. Some government departments or law enforcement agencies may release their own data related to specific predicates; these data will typically need to be compiled manually by the researchers conducting the national risk assessment, as that data may not be presented in one comprehensive source.

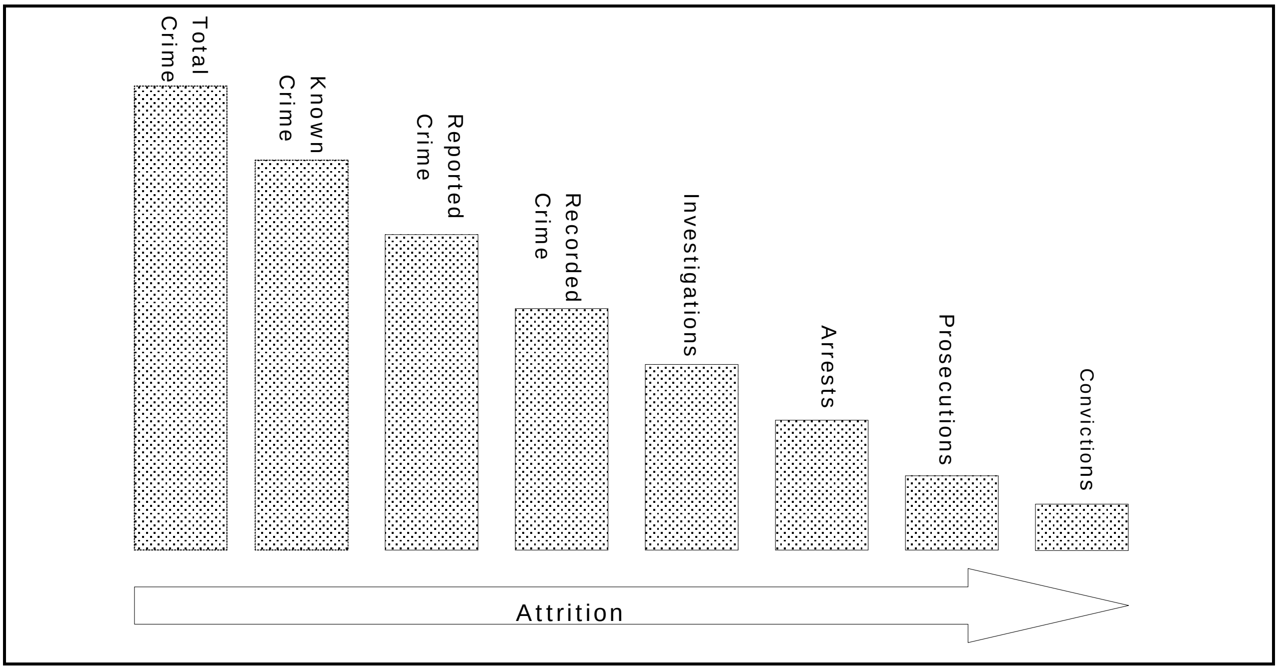
[30] Official crime statistics (including some information on the capacity of the criminal justice system) of most jurisdictions are also reproduced in the *United Nations Survey of Crime Trends and Operations of Criminal Justice Systems* (www.unodc.org/unodc/en/data-and-analysis/Crime-Monitoring-Surveys.html).

[31] Statistics may also, though less frequently, refer to the *prevalence* of crime, which refers to the proportion of people/businesses/cars/etc. in a specific area that are victimised; *concentration* refers to the number of victimisations per victim; and thus *incidence* is the product of the two. The terms *magnitude*, *scope*, and *scale* are also used variously, depending on context, to refer to total volume or total value of crimes or crime losses. Data are occasionally produced which relate to volumes of fraud losses which have been prevented, as opposed to losses that occurred. Care should be taken to ensure such data are interpreted correctly. *Impact* generally refers to the monetised costs of crime and includes losses, costs in anticipation, and costs in response in response to crime.

[32] For certain crime types, such as fraud, victims may not be aware that they have been defrauded.

[33] This may occur because the crime is viewed as difficult to prove, and the additional charge may be seen as unnecessary if a successful case can be made proving the predicate crime.

Figure 2. Attrition in Crime Data (note: not to scale)



Victimisation Surveys

115. Victimisation surveys complement official crime data, adding another dimension to measuring the incidence of crime. Victimisation surveys are typically carried out by a jurisdiction's public sector entities (*e.g.* a ministry of justice or census bureau). In victimisation surveys, members of a representative sample of the population of interest are queried about their experience(s) as victims of crime, not all of which will have been reported to law enforcement.

116. Victimisation surveys can suggest the scale of under-reporting of crime incidents, and are sometimes preferred by researchers to official crime statistics in understanding underlying crime trends. Victimisation surveys can also illustrate repeat victimisation in which the same person is repeatedly the victim of the same or different types of crime. Most common data points include information on the volume of both reported and unreported crime; information on the victims themselves and the impact of their victimisations (*e.g.* value of losses); and information on offenders.

117. As with official crime statistics, victimisation surveys have their own limitations. For example, respondents may not fully understand what information is requested in the survey (*e.g.* type of crime); and/or they may lie/exaggerate/under-/over-estimate the number of times they have been victimised (and/or the nature of the victimisation) in the period under review.

118. Of course, victimisation surveys relate to crimes with victims and are of little use in capturing data on largely so-called victimless crimes, which make up a considerable proportion of the FATF 20+ predicates. The standard victimisation surveys are focused more on crimes of violence with individuals as victims, not businesses. This is changing, and several jurisdictions (as well as the United Nations) now run commercial crime/business crime victimisation surveys. Lastly, many the 20+ crimes categories of interest here represent, in absolute terms, fairly rare events, so sample sizes in both individual and commercial/business surveys need to be large enough or such crimes will be under-represented in the findings.

Offender Surveys

119. Surveys are also used to gain an understanding of the criminal behaviour of the general public as well as incarcerated individuals. Offender surveys, like victimisation surveys, are typically carried out or sponsored by public sector entities (*e.g.* a ministry of justice or census bureau). In offender surveys, members of a representative sample of the public are queried about their experience(s) as perpetrators of crime. Not all of the self-admitted crimes picked up in these surveys will have been captured in official statistics.

120. Most common data points include information on the volume and type of offenses carried out over a certain period of time, as well as information on the respondents. These self-report surveys are also used to explore the prevalence of drug use. Data captured in these surveys can then be compared to official statistics and victim survey results to identify underlying crime trends.

121. As with victimisation surveys, offender surveys are subject to the respondent's truthfulness, understanding of the survey questions, and ability to recall relevant information. Most offender surveys to date have focused on crimes of violence and drug use.

Other Relevant Data Sources for a Threat Assessment

122. While official crime statistics commonly relate to select crime categories, there are other relevant data streams collected by various public sector entities. These data will most often have been collected by more specialised law enforcement and regulatory agencies (*e.g.* the federal or national police, the customs service, the immigration service, specialist anti-drug and anti-fraud bodies, health authorities, financial regulators, etc.; and some international bodies, including the United Nations Drug Control Program).

123. None of these data streams is perfect, and each has limitations not dissimilar to those set forth above in the section on traditional measures of crime. But these data can be of great use in understanding the ML/TF threat.

124. Case research, *i.e.* qualitative and quantitative research on specific investigations, prosecutions, or convictions can provide useful information on a sample of cases processed by law enforcement or indeed the whole criminal justice system. For example, case debriefs of a sample of convicted offenders can illustrate per-offense criminal proceeds, money laundering methods, favourite laundering jurisdictions, etc.

125. The media can be a source of qualitative and quantitative crime data. Media information must be interpreted with care, as facts may not be correct and information may not be presented in context.

126. Special mention should be made of covert or classified sources of data on crime. A number of jurisdictions count transnational crime as a national security issue, and consequently a remit of the intelligence community (IC). Thus, IC data may contribute to the understanding of threat at a national level. Classified and otherwise restricted sources of information may inform both qualitative and quantitative indicators of threat. The use of such information may enrich a threat assessment or overall risk assessment, but may require security-cleared staff and secure facilities in the preparation of the assessment.

127. Perceptions surveys reach to subsets of the population to explore facets of crime, impacts of crime, or specific crime types. Of greater relevance to money laundering threat, however, is the work of Transparency International (TI) on corruption[34]. TI employs an indirect approach to measuring corruption, by drawing on primary sources that survey business people. TI forms a corruption perception index based on the input of these sources.

[34] www.transparency.org/

128. The benefit of using perception surveys is that corruption is a crime very likely to be under-represented in crime data; the perceptions of experts can overcome this undercounting. The downside, of course, is that the results are based on opinion alone. Perception surveys are also used to gauge foreign and domestic investors' and CEOs' perceptions of crime in certain jurisdictions.[35]

129. Private sector trade and professional organisations as well as non-governmental organisations often collect data relevant to determining the ML/TF threat. These bodies, particularly those that represent or work with retailers and financial services companies, will collect crime statistics from their member organisations. This data may include information on losses due to crime.

130. The data sources above represent *micro* indicators. *Macro* indicators are estimates of the size of the shadow or criminal economy. Macro indicators build on discrepancies between expected and actual levels of demand for currency, size of the labour force size, or electricity use. Macro indicators are often criticised as being too imprecise to provide policy makers with useful information.[36] This topic is dealt with in more detail in Appendix 3.

131. Relevant qualitative data would address the status of a specific jurisdiction as being a source country or in a source region for illegal narcotics or precursor chemicals, or other high-demand illegal materials. Alongside or even in the absence of other data, this information can highlight potential sources of concern.

132. On their own, the various data points discussed above may not prove so useful, not least given deficiencies in data quality. But these data should add value in the aggregate. Levi and Maguire suggest in a 2004 paper on organised crime:

> *Success in such a strategy could be assessed by means of a 'basket' of organised crime indicators, derived from a mix of victimisation surveys, self-report studies, 'mystery shopping' (offering laundering and other crime opportunities to test control and reporting mechanisms), customs and excise evasion data, vice data, drug price data, fraud statistics, laundering cost data, and car export data (which need to be improved). While none is reliable individually, such indicators may together give us a composite portrait which reflects the complexity of what enterprise criminals are doing and provides a credible picture of trends.*[37]

133. A jurisdiction should try to understand, as broadly as possible, the threat posed by all of its relevant predicate offenses. While it will not be possible to generate indicators for all of the concepts of interest, it is important to note when a raft of indicators is not collectively exhaustive. For example, different data sources may suggest the volume and value of different predicates contributing to the money laundering threat, but it is likely that there will not be usable data for *all* of the predicates. This data deficiency must be acknowledged, lest indicators be misinterpreted. For example, deficiencies in the data for a particular type of crime might be interpreted as being indicative of little or no crime of that type in the jurisdiction.[38]

Country and Sector ML/TF *Vulnerability*

134. Understanding weaknesses in AML/CFT systems and controls, and the other aspects of a jurisdiction that make it attractive to money launderers and terrorist financiers is an important element of a national ML/TF risk assessment. The RBA paper identifies factors that may influence the ML/TF risk in a county and suggests to assess, among other things, the political and legal environment;

[35] See, for example, World Economic Forum 2007, at www.weforum.org/en/index.htm.

[36] Reuter and Truman (2004).

[37] Levi, M., Maguire, M., (2004).

[38] Of course, data deficiencies can be dealt with in various ways, *e.g.* by making various assumptions to impute missing data.

characteristics of the economy as well as the financial sector; ownership structure, integrity and corporate governance of financial institutions; types of products and services offered and clients served; and criminal activities and proceeds of crime generated domestically as well as generated abroad but laundered domestically.[39]

135. Financial institutions learn either directly from their own experience or indirectly through public sector guidance about indicators of illegal or unusual conduct and which factors make those indicators more or less likely to occur (*i.e.* customer characteristics, transaction types, and countries of concern). These indicators of unusual or criminal activity are used to establish both automated and manual screening and reporting procedures. Often the indicators used are intended to flag both what is believed to be actual illicit conduct (*i.e.* transaction structuring[40]) as well as activity that may be illicit (*i.e.* any transaction considered unusual for the customer).

136. Regulatory and supervisory authorities have the benefit of seeing across a number of financial institutions, assessing the industry's risk awareness and associated policies and procedures. Supervisors can also assess whether AML/CFT measures associated with products and services offered and clients served by financial institutions are adequate and proportionate to underlying or potential ML/TF risks.

137. Data and observations, both retrospective and prospective, from regulatory and supervisory authorities and the FIU should be fed into the national ML/TF risk assessment process. The retrospective data is drawn from the financial community's currency and suspicious transaction reporting, which provides a basis to determine how often certain criminal or unusual transactions appear, and from law enforcement investigations and prosecutions. Figure 3 illustrates the AML/CFT information flow between the public and private sectors. This information should be available to the ML/TF risk assessment process. As noted in the table, this information will be both quantitative and qualitative in nature, and represents only some of the information sources available.

138. The FIU is capable of aggregating and analyzing currency and suspicious transaction reporting. This information can also be used to assess the implementation of the AML/CFT regime, its risk awareness, and the adequacy of the associated policies and procedures. Feedback from competent authorities can help financial institutions fine-tune their risk awareness.

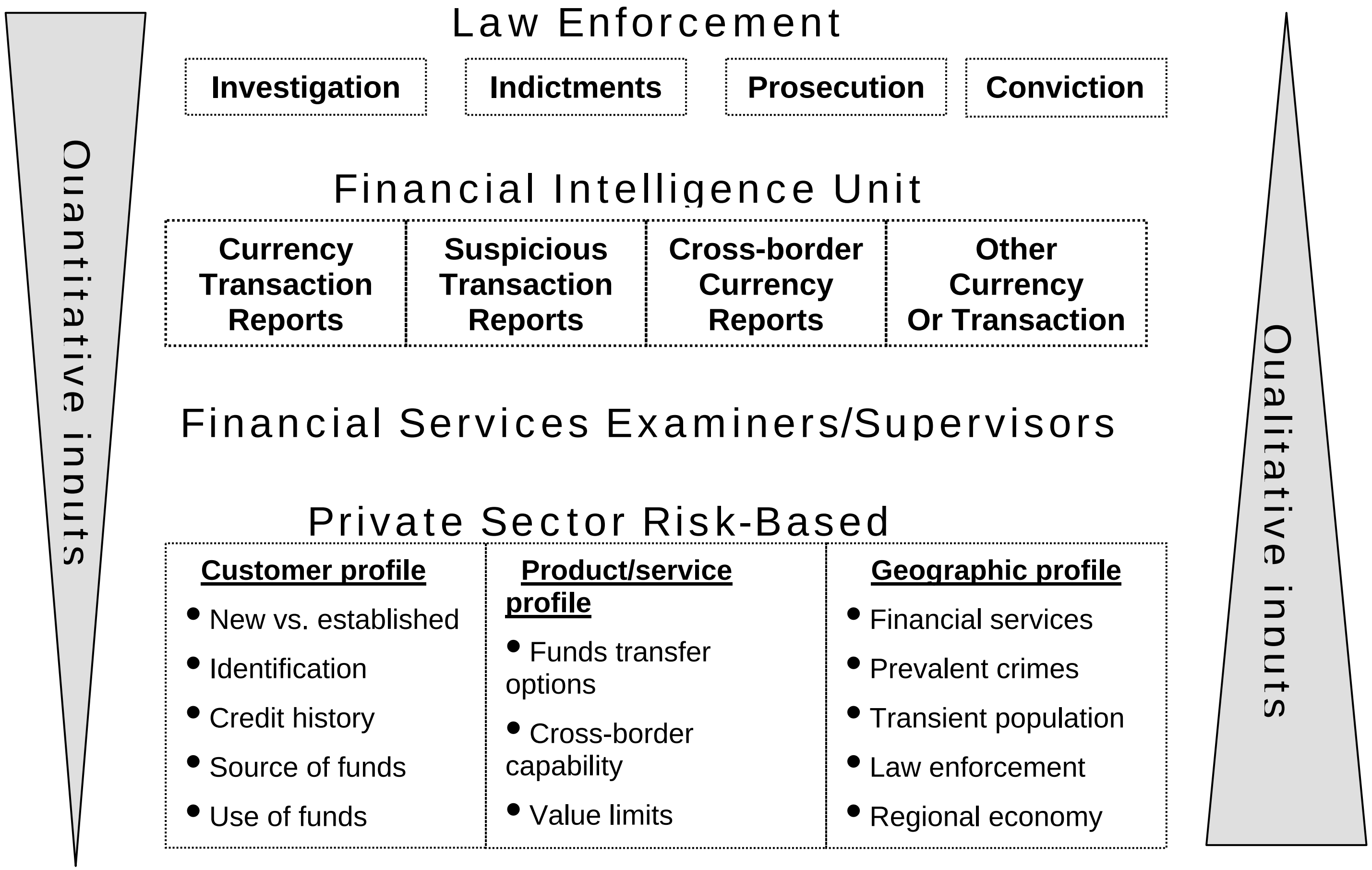
139. Comparing data from financial institutions with law enforcement data from criminal investigations and prosecutions provides what can be a complementary composite of what the public and private sectors are able to document regarding the ML/TF situation. The data and perceptions of supervisory and regulatory authorities, the FIU, and law enforcement are important inputs to determine vulnerabilities in the ML/TF environment.

140. Evaluating effectiveness is an important exercise to minimise vulnerabilities of financial institutions to money launderers and terrorist financiers. See Appendix 2 for more information on evaluating law enforcement effectiveness.

[39] FATF (2007a).

[40] Structuring involves breaking up a single large currency transaction into several smaller transactions in an attempt to evade a transaction report being filed by the financial institution with the relevant authorities.

Figure 3. Some of the public and private sector entities with relevant data, both qualitative and quantitative, for a national ML/TF risk assessment. Additional information sources include asset seizure and forfeiture data and data from customs seizures and interdictions at the border.



V. ISSUES FOR FURTHER CONSIDERATION

141. It would be desirable for jurisdictions to adopt similar definitions and concepts when conducting a national money laundering assessment. Similar approaches would facilitate the aggregation of results into a worldwide picture as well as allow jurisdictions to compare their situation with their peers.

142. FATF Recommendations 31[41] and 32[42] address the two essential factors underlying a jurisdiction's capacity to conduct a national ML/TF risk assessment: cooperation among the relevant authorities and appropriate data.

143. In addition to the information collected by the FIU from the financial community, jurisdictions should consider tracking the money laundering and terrorist financing method associated with law enforcement investigations. But this information is not usually maintained in a comprehensive fashion. Instead, competent authorities seeking this information typically must rely on the recollections and anecdotes of those involved in investigations and the occasional official public statement calling attention to a particular case.

144. Most often today compiling the relevant information available into a coherent statement of the threat posed by specific money laundering and/or terrorist financing methods requires competent authorities to agree on what is essentially a qualitative assessment based on imprecise information.

145. It may be useful for the FATF to consider pursuing best practices guidance regarding Recommendations 31 and 32 to provide additional clarity to the methods that can be used to keep track of data relevant to a ML/TF risk assessment and how competent authorities in some jurisdictions are able to cooperate and coordinate their risk assessment efforts.

[41] "Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing."

[42] "Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation."

CONCLUSION

146. Few countries currently attempt to understand their domestic money laundering or terrorist financing situation by undertaking a national ML/TF risk assessment. Those that do apply various methodologies and may focus on more than money laundering or terrorist financing (*e.g.* organised crime). While there is not an established methodology or even vocabulary for a national ML/TF risk assessment, there are good practice standards that can be identified for statistical analysis and useful lessons that can be applied from the countries that have attempted a ML/TF risk assessment.

147. Public sector supervisory authorities cannot realistically assess the private sector's implementation of a risk-based approach to combating money laundering and terrorist financing without first themselves understanding the underlying risks and necessary safeguards. In fact, financial institutions may look first to their competent authorities for guidance in identifying, assessing, and combating ML/TF threats. This reinforces the need for periodic ML/TF risk assessments produced either as a single assessment by the national government or separate assessments produced by each relevant authority.

148. Given varying national circumstances, there may not be a single format or methodology appropriate for all countries. Rather than seeking to oblige FATF members to follow a set process, this document sought to supply information for countries to consider when developing their own ML/TF risk assessment. Further, it is hoped that the document will help to increase the number of countries producing national assessments. Not only will this be of use to national authorities, but it will also allow countries to participate more effectively in FATF exercises (*e.g.* annual typologies exercises). The long-term effect will be to enhance knowledge at the national and international levels.

149. Combating money laundering and terrorist financing requires an ongoing understanding of the methods used by criminals to launder their illicit funds and fuel terrorism. These methods range from well-known practices established over many years to modern techniques that exploit innovations in global payment networks as well as the Internet. By maintaining an awareness of current money laundering and terrorist financing methods and conducting a threat or risk assessment addressing the methods observed domestically and within the region, a country will facilitate *i)* efficient AML/CFT resource allocation; *ii)* compliance with the FATF recommendations; *iii)* practical risk-based examination and supervision of domestic financial institutions; and, *iv)* the ability to monitor the effectiveness of domestic AML/CFT laws, oversight, and enforcement.

150. All countries are faced with the challenge of allocating scarce resources to fund AML/CFT programs and other public policy and safety efforts. In the budgeting process it is important to identify and prioritise issues that require the most immediate attention. This process requires an understanding of the money laundering and terrorist financing threats relevant to the country's economy and financial institutions. An analytically sound risk assessment using valid inputs can help governments make decisions about how to target investments and set priorities for industry oversight and law enforcement.

BIBLIOGRAPHY

Carrol, L. (2007), “Alternative remittance systems distinguishing sub-systems of ethnic money laundering in INTERPOL member countries on the Asian continent”, INTERPOL website, *www.interpol.int/Public/FinancialCrime/MoneyLaundering/EthnicMoney/default.asp*.

Commission for the Prevention of Money Laundering and Monetary Offences (CPBC) (2004), *Annual Report*, Madrid, *www.sepblac.es/ingles/acerca_sepblac/acercade.htm*

Dean, W. Lee, (2007), *Program Evaluations: Improving Program Effectiveness and Organisational Efficiency*, FBI Law Enforcement Journal, Vol. 76, No. 11, accessed at: *www.fbi.gov/publications/leb/2007/nov07leb.pdf*

EUROPOL (2007), *Organised Crime Threat Assessment*, Europol, The Hague, *www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA2007.pdf*

FATF, (2008), *Terrorist Financing Typologies*, FATF, Paris, www.fatf-gafi.org.

FATF, (2007a), *Guidance on the Rick-based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*, FATF, Paris, www.fatf-gafi.org.

FATF, (2007b), *AML/CFT Evaluations and Assessments: Handbook for Countries and Assessors*, FATF, Paris, www.fatf-gafi.org.

The *FATF Forty Recommendations* and the *Special Recommendations on Terrorist Financing* are available through the FATF web site: www.fatf-gafi.org.

HM Treasury, (2007), *The Financial Challenge to Crime and Terrorism*, HM Treasury, London, *www.hm-treasury.gov.uk/media/C/B/financialchallenge_crime_280207.pdf*.

Jost, Patrick and Harjit Sandu (2000), “The hawala alternative remittance system and its role in money laundering”, INTERPOL website, *www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp*

Levi, Michael and Mike Maguire (2004) “Reducing and preventing organised crime: An evidence-based critique”, *Crime, Law and Social Change*, Vol. 41, No. 5, Heidelberg.

Money Laundering Threat Assessment Working Group (U.S. Department of the Treasury, *et al.*) (2005), *U.S. Money Laundering Threat Assessment*, U.S. Department of the Treasury, Washington, DC, *www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf*

Painter, Kate A. and David P.Farrington (2001), *The financial benefits of improved street lighting, based on crime reduction*, Lighting Research and Technology, Vol. 33, No. 1, 3-10. Accessed at: *http://intl-lrt.sagepub.com/cgi/content/short/33/1/3*.

Reuter, Peter and Edwin M. Truman (2004), *Chasing Dirty Money*, Institute for International Economics, Washington, DC.

Serious Organised Crime Agency (SOCA) (2006), T*he United Kingdom Threat Assessment of Serious Organised Crime*, SOCA, London, *www.soca.gov.uk/assessPublications/downloads/threat_assess_unclass_250706.pdf*.

SOCA (2006), Review of the Suspicious Activity Reports Regime ("The SARs Report"), SOCA, London, *www.soca.gov.uk/downloads/SOCAtheSARsReview_FINAL_Web.pdf*.

Transparency International, www.transparency.org.

Unger, B. *et al.* (2006), *The Amounts and Effects of Money Laundering*, Ministry of Finance, The Hague, *www.minfin.nl/binaries/minfin/assets/pdf/actueel/bijlage-nieuwsberichten/2006/02/06-011a.pdf*.

United Nations Office on Drugs and Crime, *Crime Surveys*, *www.unodc.org/unodc/en/data-and-analysis/Crime-Monitoring-Surveys.html*.

U.S. Department of Justice (2006), *Crime in the United States, 2006*. Federal Bureau of Investigation web site, *www.fbi.gov/ucr/cius2006/documents/aboutcius.pdf*.

World Economic Forum 2007 website www.webforum.org/en/index.htm.

APPENDIX 1: SUMMARY OF MONEY LAUNDERING ASSESSMENT SURVEY RESPONSES

This annex summarises key observations based on information provided by jurisdictions to the project survey questionnaire. The respondents did not necessarily answer all questions in some cases. In total, 15 jurisdictions responded to the survey questionnaire.

It is important to note that the project team deliberately phrased the survey questions broad with a view to capture as much information as possible. For example, jurisdictions may be undertaking some type of a national assessment which may be similar to threat or other type of national assessment, although it may not be called a "threat assessment." This is reflected in the broad range of responses summarised below.

The purpose and scope of the questionnaire was explained as shown in the box below.

PURPOSE AND SCOPE

This survey is intended to collect information concerning how jurisdictions determine priorities, develop strategies, and allocate resources to support anti-money laundering (AML) efforts. The survey also seeks information on the terms and concepts jurisdictions use in their risk analysis. Although the survey refers interchangeably to risk, threat, and vulnerability, this usage is provisional pending the results of the survey and further research by the FATF WGTYP MLTA project team.

The survey is limited to questions regarding how money laundering threats are identified and how AML initiatives are evaluated. This approach addresses both financial crime and to a large extent efforts to combat the financing of terrorism (CFT). To consider how jurisdictions identify and prioritise a broader range of terrorist financing threats (including the use of legitimate funds and state sponsors), and the methods used to evaluate CFT effectiveness in that broader context, is beyond the scope of this project.

The MLTA Project Team intends to use the information collected in the survey along with information from other sources, to propose guidance that will assist jurisdictions in developing methodologies to *i)* identify and prioritise money laundering threats, *ii)* apply consistent risk analysis terms and concepts, and *iii)* coordinate multilateral AML/CFT strategic planning.

Subsequently, three broad questions were asked with regards to threat assessment, program effectiveness, and terms and concepts. Responses by jurisdictions are summarised in each question.

A) Threat Assessment

All jurisdictions prioritise AML efforts directly or indirectly through the allocation of personnel and financial resources. The questions in this section, however, ask whether a money laundering threat assessment is conducted independent of the budgeting and personnel management processes.

A.1. Have one or more offices of the national government attempted a formal effort to identify and assess the use of all relevant money laundering methods exploited to move illicit funds into, out of, or within the jurisdiction?

YES	11 jurisdictions		NO	4[43] jurisdictions

If YES, please describe the following in as much detail as possible:

A.1.a Objective of the threat assessment:

Main objectives of the threat assessment vary from jurisdictions to jurisdictions. Broadly speaking objectives can be categorised as follows:

ML Typologies
To identify and monitor ML methodologies/techniques, trend and typologies

Nature, Size and Effects of ML
To obtain better information on size, flow and effects of ML on economy
To understand the relative impact and size of ML vis-à-vis other criminal phenomena,

Predicate Crimes
To identify nature, size, impact and trend of organised crime
To identify source of funds so as to deter ML

Sector ML Risk
To identify risk indicators (whether particular products and services or others) for financial sectors and other covered businesses and professions
To understand the impact of ML on financial sector so that proportionate counter-measures are determined
To assess vulnerability of specific sectors

Policy Planning
To set priorities for AML measures
To provide inputs for AML policy planning

A.1.b Methodology of the threat assessment:

Methodologies for the threat assessment also vary from jurisdictions to jurisdictions. While some jurisdictions provided detailed methodologies of their assessment (especially based on economic modelling), other jurisdictions provided a broad approach to the threat assessment.

Broadly speaking methodologies can be categorised as follows:

Economic Model
John Walker Model

Qualitative and Quantitative Analysis Based on:
Expert Survey
Survey of law enforcement agencies, experts and FIU

FIU or Law Enforcement Data
Analysis and examination of FIU data
Develop indicators based on police and FIU data
Establish patters in amounts, destinations, explanations, etc.

Research
Assessment of relevant studies and reports by government agencies, research institutes, among others.

Laws and regulations
Analysis of laws and regulations to determine safeguard adequateness to understand the level of vulnerability

[43] One jurisdiction did not clearly answer this question. The rest of questionnaire response provided by this jurisdiction indicates that a framework is in place to conduct a national assessment; however, no assessment appears to be undertaken to date. Thus it is counted towards not having undertaken a threat assessment.

A.1.c Nature and sources of information used in the threat assessment:

A number of information sources are consistently used for national threat assessments:

- Operational sources
- Conviction information
- Database information- STRs, CTRs
- Specific intelligence gathering operations
- International information- Interpol/Europol assessments, FATF Typologies
- Financial and economic information
- Private Sector information
- Academic/Public research
- Media

A.1.d Public and private sector offices participating in the threat assessment:

Depending on assessment type or model, or its objectives, public and private sector offices involved in the threat assessment vary. Some jurisdictions undertake a multi-agency threat assessment, while some undertake a single agency based threat assessment.

Jurisdictions listed law enforcement agencies, FIU, regulatory bodies as well as policy making bodies having a critical role in the threat assessment. In some cases, private sector offices, academic or research institutes and other experts are also brought in.

A.2. (a) If the answer to question A.1 is NO, are there plans to initiate a formal money laundering threat assessment in the next 12 months? If NO, please describe why a money laundering threat assessment is not necessary or not feasible in your jurisdiction.

(b) If the answer to question A.1 is YES, how often are such threat assessments conducted and how are the results used?

Those jurisdictions that currently do not carry out a national assessment indicated that they plan to initiate one soon.

Those jurisdictions that currently carry out a national assessment indicated that it is undertaken on an annual basis if it is an assessment that is or similar to typologies exercise. Other types of national assessments are undertaken periodically although the time span varies depending on the need and available resources.

B) Program Effectiveness

The questions in this section concern how AML efforts are evaluated. The relative significance of any specific money laundering threat is influenced by the effectiveness of AML programs. Answers should be based on whatever processes a jurisdiction has in place which may require AML program effectiveness to be measured (*e.g.* budgeting, personnel management, or policy development).

B.1. Have one or more offices of the national government attempted to assess the "effectiveness" of domestic AML efforts – either narrowly, to evaluate a specific program or initiative, or more broadly?

YES	13 jurisdictions	NO	2 jurisdictions

If YES, please describe the following in as much detail as possible:

B.1.a Purpose of the AML effectiveness evaluation(s):

Assessment of AML effectiveness is used to evaluate an AML regime both at the high-level to determine overall national policy and at the lower-level to determine whether specific objectives were met. Key observations of the purpose of AML effectiveness evaluation are:

To review performance of programs and their efficiency from a budgetary point of view to make informed decision on prioritisation
To examine progress of AML regime and set objectives for the future
To minimise threat, vulnerability and consequent risk to financial sector and other economies.
To assess whether the performance met specific objectives (for example, registration of MSBs, creation of supervisory bodies, etc.)
To determine whether the risk management framework was appropriately designed to promote detection and deterrence of ML
To assess presence of safeguards against identified threats

In a couple of jurisdictions, evaluation on effectiveness is mandated, for example, on regulatory measures or institutions such as an FIU.

B.1.b Definition of "effectiveness" used in the evaluation process:

The term, effectiveness, is often used in different circumstances, thus defining effectiveness cannot be isolated from the circumstances in which the term is used.

Jurisdictions shared the following use of the term. Effectiveness can be measured based on
whether the set objectives (including scope and measures) have been met
whether the law has been enforced
whether the measures in place have resulted in confiscation, reporting of STR and CTR
whether public policy initiatives or law enforcement actions resulted in a perceived shift in ML activity
efficiency in processing information by obligated institutions

B.1.c Nature and sources of information used in the evaluation process:

Information source for assessment of effectiveness is in principle quite similar to that of threat assessment. However, more emphasis is placed on legal, regulatory and compliance information.
Domestic laws and regulations
FATF 40+9 Assessment Methodology
Regulatory compliance reports
FIU information (STR, CTR)
Interview with experts and witnesses
Conviction information
Data on frozen assets
Cases forwarded to law enforcement agencies

B.1.d Quantitative or qualitative method used to measure effectiveness:

In most jurisdictions, both quantitative and qualitative methods were used to measure effectiveness based on information and data specified in section B.1.c.

For example, quantitative methods include statistical analysis on STRs, number of cases under prosecution, amount of money laundered, amount of assets seized and confiscated, and other financial intelligence data. Qualitative methods include analysis on treat and methods of ML, adequacy of safeguards, interviews of experts and officials to determine whether objectives were met.

B.2. (a) If the answer to question B.1 is NO, are there plans to begin evaluating AML effectiveness for budgeting, personnel management, or policy development, in the next 12 months? If NO, please describe why evaluating AML effectiveness is not necessary or not feasible in your jurisdiction.

(b) If the answer to question B.1 is YES, is AML effectiveness evaluated as part of an overall money laundering threat assessment?

Jurisdictions that are currently not carrying out evaluation of effectiveness did not indicate that they plan to do so within the next 12 months.

The response to whether the AML effectiveness is evaluated as part of an overall ML threat assessment was divided. Five jurisdictions answered that evaluation of effectiveness is part of threat assessment while four jurisdictions answered it is not part of threat assessment. Other did not respond to this question.

C) Terms and Concepts

C.1. The terms "risk," "threat," and "vulnerability" are often used interchangeably when considering the potential harm of specific money laundering methods and the effectiveness of AML safeguards. Has your jurisdiction agreed on a consistent approach to applying these or other terms? If so, please list the relevant risk management terms or concepts and describe how they are used in your jurisdiction.

No respondent offered a set of consistent definitions for these terms in the ML context. Six jurisdictions indicated that there is no consistent approach to the use of the terms. Two jurisdictions kept this space blank. The rest of seven jurisdictions provided their understanding of the terms as these terms are frequently used in AML.

APPENDIX 2: EVALUATING LAW ENFORCEMENT EFFECTIVENESS

151. Assessing a nation's vulnerability to money laundering and/or terrorist financing, whether undertaken broadly at the national level or more narrowly, should include a consideration of whether current AML/CFT safeguards are adequate. Money launderers and financiers of terrorism seek out jurisdictions and financial systems where AML/CFT practices are weak and ineffective, which makes inadequate AML/CFT efforts a potential indicator of money laundering and terrorist financing risk.

152. Countries may allocate significant resources to implementing and enforcing AML/CFT laws, but find it difficult to demonstrate that their efforts are having an impact. While preventative efforts may not immediately eliminate financial crime, money laundering, or terrorist financing they should have a discernible effect.

153. FATF mutual evaluations, which assess a country's implementation of the FATF Recommendations and Special Recommendations, require assessors to determine "whether the required measures have been properly and effectively implemented, and that the system is effective."[44] To demonstrate that the country's AML/CFT efforts are having an impact on financial crime, money laundering, or terrorist financing may require not only statistics, but also qualitative information, potentially anecdotal. But this information can be collected and organised systematically.

154. Demonstrating a cause-and-effect relationship between AML/CFT efforts and crime statistics is almost impossible because of the many factors that influence the level of crime, money laundering, and terrorist financing in a jurisdiction. Among the factors listed by the U.S. Federal Bureau of Investigation (FBI) are[45:]

- Population density and degree of urbanisation.
- Variations in composition of the population, particularly youth concentration.
- Stability of the population with respect to residents' mobility, commuting patterns, and transient factors.
- Modes of transportation and highway system.
- Economic conditions, including median income, poverty level, and job availability.
- Cultural factors and educational, recreational, and religious characteristics.
- Family conditions with respect to divorce and family cohesiveness.
- Climate.

155. The FBI also lists:

- Effective strength of law enforcement agencies.
- Administrative and investigative emphases of law enforcement.

[44] FATF (2007b), p. 10.

[45] U.S. Department of Justice (2006).

- Policies of other components of the criminal justice system (*i.e.* prosecutorial, judicial, correctional, and probational).
- Citizens' attitudes toward crime.
- Crime reporting practices of the citizenry.

156. Isolating the impact of each of these factors defies easy or objective measurement. "For example, one city may report more crime than a comparable one, not because there is more crime, but rather because its law enforcement agency through proactive efforts identifies more offenses. Attitudes of the citizens toward crime and their crime reporting practices, especially concerning minor offenses, also have an impact of the volume of crimes known to police."[46]

157. Researchers have shown that with certain crimes, the impact of law enforcement initiatives can be studied effectively by focusing narrowing and limiting the geographic scope of the study. Two research projects in the United Kingdom studied the effect of improved street lighting on crime in the communities of Dudley and Stoke-on-Trent. Both studies were able to demonstrate that the improved lighting reduced crime and that the new lighting was cost effective.[47]

158. Unlike the U.K. street lighting studies assessing the impact of AML/CFT initiatives may not yield direct evidence of reduced crime or terrorism. AML/CFT initiatives, particularly law enforcement efforts, may involve many intermediary stages and accomplishments, which may ultimately lead to a measurable reduction in money laundering, financial crime, or terrorism. Table 2 illustrates an FBI model for diagramming a generic law enforcement departmental assessment program.[48] The model illustrates that following the initial program inputs and activities there are a number of intermediate steps before the long-term goal of reduced crime can be achieved.

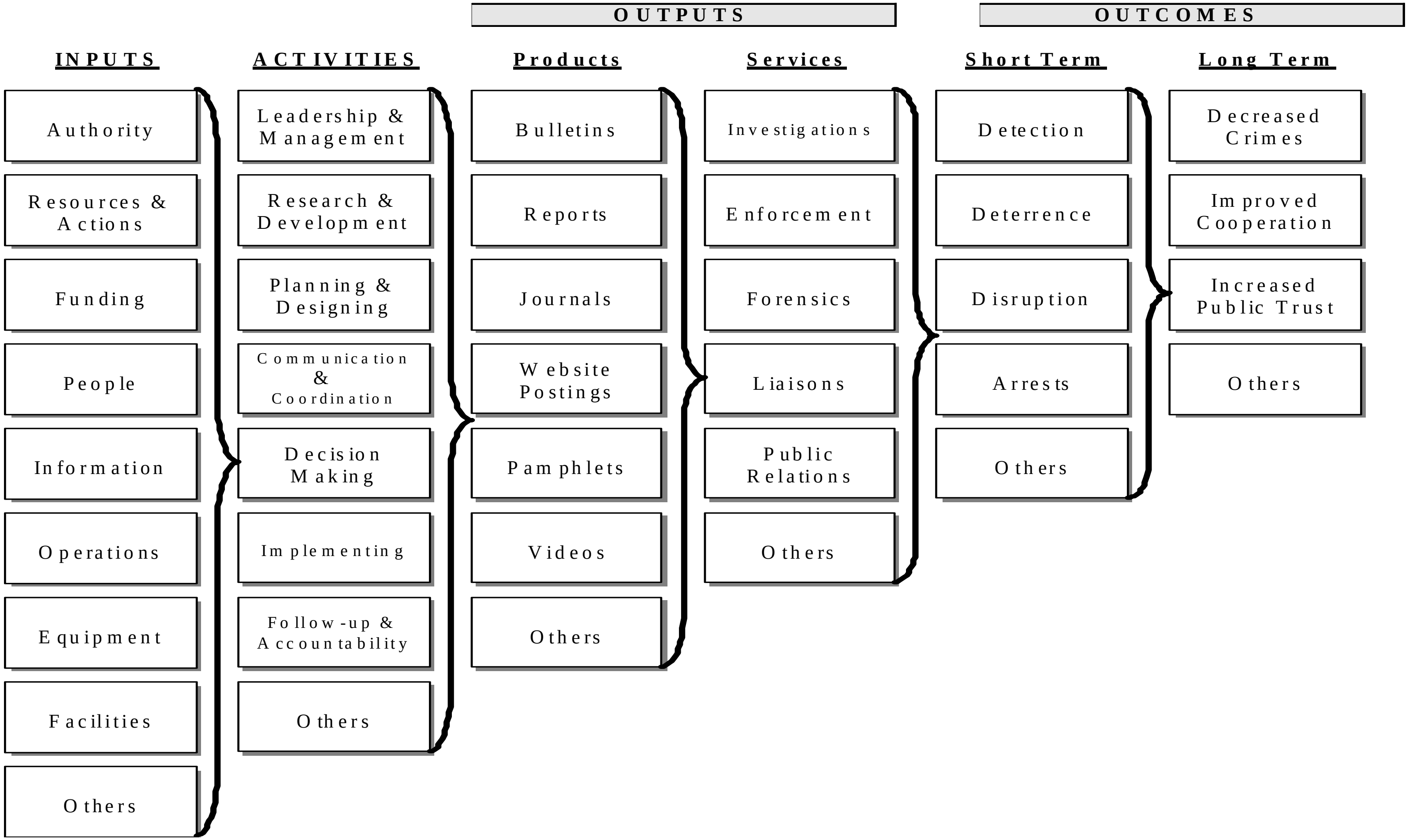
159. When assessing AML/CFT program effectiveness, it is important to identify the incremental steps in what is typically a long-term effort. Rather than attempting to draw an immediate connection between initial inputs and long-term outputs, look for incremental accomplishments, measured either quantitatively or qualitatively. The goal is to determine whether the incremental results are significant in themselves and whether they indicate that the program is making progress toward long-term goals.

[46] *Ibid.*

[47] Painter and Farrington (2001).

[48] Dean, W. L., (2007).

Table 2 A. generic law enforcement effectiveness assessment process (*Source*: U.S. Federal Bureau of Investigation)



		OUTPUTS		OUTCOMES	
INPUTS	ACTIVITIES	Products	Services	Short Term	Long Term
Authority	Leadership & Management	Bulletins	Investigations	Detection	Decreased Crimes
Resources & Actions	Research & Development	Reports	Enforcement	Deterrence	Improved Cooperation
Funding	Planning & Designing	Journals	Forensics	Disruption	Increased Public Trust
People	Communication & Coordination	Website Postings	Liaisons	Arrests	Others
Information	Decision Making	Pamphlets	Public Relations	Others	
Operations	Implementing	Videos	Others		
Equipment	Follow-up & Accountability	Others			
Facilities	Others				
Others					

APPENDIX 3: ESTIMATING THE TOTAL SCOPE OF MONEY LAUNDERING

160. The accuracy of estimates of the amount of money in need of laundering in a jurisdiction (*i.e.* the threat) may be questionable at best. This document does *not* seek to answer the question: "how much money is laundered in jurisdiction X or in the world." Rather, the objective is to focus on data points which are suggestive or indicative of the domestic and international threat, not perfectly reflective of the magnitude of that threat. As such, the focus here is on data pertaining to:

- Domestic predicate offenses.
- International predicate offenses, where appropriate (*e.g.* relating to the number of international law enforcement requests for cooperation made to/from each jurisdiction, and also STRs).
- The openness and attractiveness of the jurisdiction to laundering proceeds, including those generated outside its borders, as attractiveness and openness can be viewed as contributing to vulnerability which increases the threat.

161. How, then, can the money laundering threat be measured? Clearly, a multi-source hodgepodge of data sources for different crimes, all with different measurement methods, is suboptimal and should be avoided.[49] But there is little doubt that indicators of threat will need to pull from disparate data streams.

162. Given that the primary goal of this exercise is to understand a jurisdiction's money laundering threat, *i.e.* its demand for laundering, the first order of business should be to employ data on crime to suggest the magnitude of the domestic proceeds generated by the predicates (which will need laundering). This is *very* difficult, if not impossible, to achieve with any certainty. It should be remembered, however, that the focus here is on *indicators* of threat (*i.e.* rough orders of magnitude to highlight issues requiring action), not precise estimates of laundering.

163. Ideally, an indicator of the *value* of domestic proceeds would represent the sum of the estimated *proceeds* for each of the relevant crime types and subtypes as appropriate (see Figure 4, which uses fraud as an example).[50] Data for at least some crime types will require the use of *loss* data (particularly for the predatory crimes) as a proxy for *proceeds*.[51] With estimated proceeds per crime type, predicate data can illustrate the relative level of proceeds they generate (perhaps leading to low/medium/high scores based on this ranking or some absolute levels); and with time series data, changes in year-on-year proceeds can indicate crimes of growing concern. For international comparisons (and to validate estimates), value data should be presented per capita and per unit of GDP.

164. It is a virtual certainty that *no* jurisdiction will be in a position to estimate the complete value (or perhaps anywhere close) of the money laundering threat in this way due to data shortages (to say nothing of sub-par data quality). But – importantly – this process can usefully illustrate what is known,

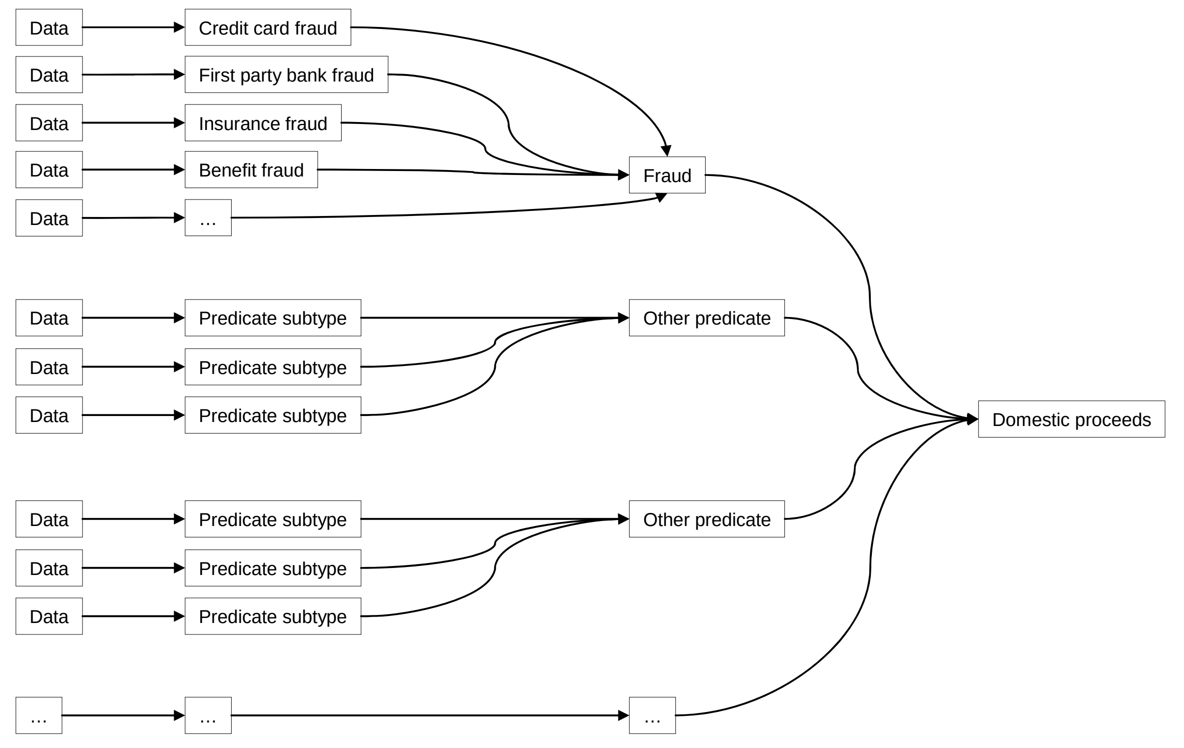
[49] See Reiss and Biderman (1980) for an extensive commentary on the challenges presented by multiple, decentralised data sources.

[50] In some jurisdictions, research has been carried out on the costs of crime to the jurisdiction, or on criminal proceeds generated therein, or the like. In this case, much relevant data may have already been compiled; indicators of threat should be informed by such research whenever possible.

[51] Some of these proceeds/losses estimates will have been derived from administrative records, like excise avoidance estimates derived from administrative data on cigarette sales compared to surveys on smoking trends.

what is not known (*i.e.* where data deficiencies lie), and where data collection and research efforts should be focused. And, much like with benefit-cost analysis (in which data deficiencies are common), policy-making here can be transparently based on existing data complemented by imputed findings and informed judgments (themselves derived from clearly spelled-out assumptions).[52]

Figure 3. Data-Driven Estimation of the Value/Volume of the ML Threat



Note: Data supporting each predicate subtype will largely, but not exclusively, draw from public- and private sector administrative data (complemented by victimisation and other data as needed). Of course, all predicates must be included in the exercise.

165. A similar exercise should be undertaken for the *volume* of reported predicate crimes.[53] Mindful of the limitations of data on reported crime (including that multiple crimes occurring at once may only be recorded as one offense), volume data can similarly illustrate relative levels and by year-on-year growth (to illustrate the predicates of greatest concern). Volume data can also be used to generate overall estimates of the value of criminal proceeds by crime type (*e.g.* in jurisdictions in which research, perhaps case research, has been carried out on the mean or median proceeds per offense by crime type). Again, it is very likely that no jurisdiction will have complete volume data, but the exercise can be of use nonetheless.

166. Other data sources can serve to suggest the robustness and rough-order-of-magnitude validity of value and volume findings, and also can otherwise fill gaps in understanding. For example:

- STRs often contain information on amounts of funds involved in suspicious transactions and activity. When viewed in aggregate this information can be used to generate a (very) rough

[52] Thanks go to Peter Reuter for the benefit-cost analysis metaphor.

[53] In understanding volume, crime reports are preferable to data on prosecutions/convictions in that reports more fully represent underlying crime trends (as opposed to enforcement activity). Also, private sector administrative data and victimisation data, which will likely contribute to the overall understanding of the volume of predicates (given deficiencies in public sector data), more closely resemble crime report data.

order of magnitude of laundering, which can subsequently be compared to estimates based on crime data. When crime type is determined in a STR by the STR filers or FIU, these aggregate data by crime type can be checked against the crime data by type; and such information can be used to generate a relative order of crimes by amounts (which can be checked against other rankings).[54] Of course, with STRs, it is important to control for the size of the reporting sector, whether or not there is a *de minimis* filing threshold, and the filtering approach used in the jurisdiction.[55]

- Trade data can be used to suggest an aggregate rough order of magnitude of potential trade-related laundering, again for comparison to any information derived from crime data.
- Shadow economy and none-observed economy (NOE) data can be used for rough order of magnitude checks against those crime types (in aggregate) that they relate to (*e.g.* enterprise crimes for NOE data), though given the weaknesses with shadow economy data in particular, less importance should be attached to this check of robustness.
- Though representing downstream criminal justice system activity, and thus an underestimate of total proceeds, data on confiscations and restitutions can be used (by appropriate crime type: enterprise for confiscations; predatory for restitutions) to check rough order of magnitude estimates. Rankings by crime type can be checked against similar rankings derived from other data.
- For jurisdictions with no data whatsoever on specific crime types, say, smuggling of gems or precious metals, useful qualitative indicators can start to fill the gap in understanding by illustrating, for example, whether or not the jurisdiction is viewed as a source country for gems, or a trading centre. This is also suggestive of the fact that there should be a flow of illicit funds involved somehow, unless *all* payments are handled offshore.

167. Other indicators may also serve to suggest the more qualitative *nature* of the ML threat. Information on the nature of the threat might include an understanding of laundering methods (and whether they change by crime type); criminal groups (and whether or not laundering appears to be being carried out by and for individuals or groups) and their capability and intent; use/placement of insiders; use of violence/intimidation; etc. Indicators of the nature of the threat are based on data held primarily by law enforcement and the intelligence community. In this case, a document focused on the nature of the threat may require restricted circulation.

168. In sum, then, the approach is as follows: multiple data streams inform the value and volume of each predicate. For predicates with value/volume data deficiencies, informed decisions can be made based on other quantitative and qualitative data sources to impute missing data (including their estimated relative importance to the demand for ML). Other data sources can also serve to validate findings, and to suggest the nature of the threat.[56]

[54] Crime types within STRs are tenuous, of course, as STR filers will often have insufficient information to determine the crimes involved, and may erroneously specify (or fail to specify) crime type.

[55] Some jurisdictions encourage STR filers to file a STR only when they are virtually sure they are witnessing laundering, whilst others encourage STRs to be filed even at only a hint of suspicion. Moreover, the degree of training for staff who submits STRs varies considerably. Controlling for the size of the filing sector and the underlying crime/laundering trends, the former jurisdiction will file fewer STRs then the latter. Also, when thinking about numbers of STRs and numbers of individuals mentioned as parties/counterparties to transactions, it is important to remember that one STR may relate to one individual; one STR may relate to multiple individuals; multiple STRs may relate to one individual; and/or multiple STRs may relate to multiple individuals. Advanced analytics methods need to be brought to bear to build networks of related STRs/individuals before thinking in terms of raw inputs and outputs.

[56] In the event, the risk (and thus associated threat) being assessed matters. If the goal is to assess the risk of the laundering of the proceeds of a particular crime type (or, more likely, to assess the risk of the laundering of all proceeds, broken out my crime type), then threat indicators should largely draw on value and volume data. If the goal is to assess the risk to the banking sector (or some other sector of the economy) of the laundering of

169. Gaining an understanding of the magnitude of the threat posed to a jurisdiction by the rest-of-world criminal profits lurking just beyond its borders is difficult. But certain indicators can suggest the interest of the countries of the world in that specific jurisdiction with regard to criminal assets, which may be held therein. A cautionary note, however, is that the indicators described below may be based to some extent on the same underlying source data – and this will not always be clear. For example, global illicit money flows research may itself draw on STRs, seizures, requests for assistance, and even media data. The focus might best be placed on requests for assistance, with the remaining indicators serving to check the robustness of findings.

170. To begin, jurisdictions worldwide make and receive requests for law enforcement assistance, as well as extradition. These include requests made between Egmont Group members, as well as requests made through formal mutual assistance channels and informal, non-Egmont, agency-to-agency requests. With data for jurisdictions worldwide (conveniently, some of these data are called for by FATF in the course of an evaluation), an understanding can be gained of a country's relative position in terms of the number of requests made to it (regarding specific crime types) by other jurisdictions in a particular year (which could be normalised somehow to represent high/medium/low international interest).[57] Also of use as an indicator is the percentage change in requests made to/from a jurisdiction year-on-year.

171. STRs may also suggest an international component to criminality, particularly laundering. In this case, STRs may contain information on suspicious wire transfers or other information suggestive of international sources/destinations, as well as amounts involved in any suspicious activity. This information can be used in aggregate to illustrate flows of suspicious funds to and from jurisdictions, and, as above, can be used to generate a relative order of jurisdictions and year-on-year changes.[58]

172. Data on volume and value of seizures (*e.g.* of contraband including drugs, and goods on which no excise is being paid; humans for trafficking and smuggling; undeclared cash; etc.) at international borders (and data on their source or destination country, depending on whether the seizure was at point of entry or exit) can indicate the international dimension of predicate criminality (though this criminality may be counted in data on domestic predicates/proceeds, so it is important to be mindful of double-counting).

173. A number of jurisdictions have independently or cooperatively embarked on global illicit money flows research (which often includes information on cash smuggling). For jurisdictions in which this is the case (and for which this research is sufficiently developed), this research can be used to indicate inflows and outflows (and source/destination countries) of criminal funds. Like with the requests for assistance, illicit money flows data can contribute to a relative ordering of jurisdictions in a particular year, as well as year-on-year changes.[59] This research and these data are likely to be restricted if not classified.

criminal proceeds, then threat indicators may draw on STRs, law enforcement case data, and data held by banks. If the goal is to assess the risk of the laundering of the proceeds of organised crime activity, then indicators may need to focus on value/volume as well as specific intelligence on the predicate offenders and launderers.

[57] Similar use could be made of INTERPOL FOPAC (money laundering-related) requests.

[58] For jurisdictions with FIUs which capture wire transfer data and/or data on the international movement of monetary instruments, advanced analytics approaches can establish relationships (including non-obvious relationships) between STRs and wire transfer/monetary instrument data (relationships which may even involve threshold-based reports, like CTRs). These approaches can enrich the understanding of the international aspect of laundering.

[59] This information may also be compared to information on the flows of licit funds to explore relationships therein.