Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid

Cahier 2017-13a

National Risk Assessment on Money Laundering for the Netherlands

H.C.J. van der Veen
L.F. Heuts

Cahier
The ‘Cahier’ series comprises concise reports of research conducted by and/or on behalf of the WODC.
Inclusion in the series does not mean that the contents reflect the point of view of the Dutch Minister of Justice and Security.

Contents

Abbreviations

ABN AMRO	General Bank of the Netherlands, Amsterdam-Rotterdam Bank
AFM	Netherlands Authority for the Financial Markets
AIVD	General Intelligence and Security Service
AMLC	Anti Money Laundering Centre
PBO	Public Benefit Organisation
BES	Bonaire, Saint Eustatius and Saba islands
BFT	Financial Supervision Office
GDP	Gross Domestic Product
BTW	Wwft Supervision Office
CBS	Statistics Netherlands
CIA	Central Intelligence Agency
CPI	Corruption Perceptions Index
DNB	Dutch Central Bank
DLR	National Investigation Service
ECOLEF	Economic and Legal Effectiveness of Anti Money Laundering and Combating Terrorist Financing Policy (Utrecht University study)
EU	European Union
ERA	External Referral Application
FATF	Financial Action Task Force
FEC	Financial Expertise Centre
FIU Netherlands	Financial Intelligence Unit Netherlands
FIOD	Dutch Fiscal Intelligence and Investigation Service
GDR	Group Decision Room
IARM	Identifying and Assessing the Risk of Money laundering in Europe (study coordinated by Transcrime)
iCOV	Criminal and Unexplained Assets Infobox
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
IND	Immigration and Naturalisation Service
ING	International Netherlands Group (bank)
SZW	Social Affairs and Employment
ISO 31000	Risk management according to the standards of the International Organization for Standardization
KNB	Royal Dutch Association of Civillaw Notaries
Ksa	Dutch Gaming Authority
LIEC	National Information and Expertise Centre
MCA	Multi-Criteria Analysis
NBA	Netherlands Institute of Chartered Accountants
NCTV	National Coordinator for Security and Counterterrorism
NDB	National Threat Assessment
NOvA	Netherlands Bar Association
NRA	National Risk Assessment
NVB	Dutch Banking Association
NVGTK	Netherlands Association of Financial Transaction Agencies
NVM	Netherlands Association of Brokers and Appraisers
OECD	Organisation for Economic Co-operation and Development
OM	Public Prosecution Service
PEP	Politically Exposed Persons

PESTLE	Context-analysis method taking Political, Economic, Social, Technological, Legal and Environmental aspects into account
RABO	*Raifeissen Bank, Boerenleenbank*
RIEC	Regional Information and Expertise Centre
SNRA	Supranational Risk Assessment
TBML	Trade-Based Money Laundering
UBO	Ultimate Beneficial Owner
US	United States (of America)
VFN	Association of Financing companies in the Netherlands
Wet Bibob	Public Administration Probity Screening Act
WODC	Research and Documentation Centre
Wft	Financial Supervision Act
WTR	Wire Transfer Regulation
Wtt	Trust and Company Service Providers (Supervision) Act
WvS	Dutch Penal Code
Wwft	Money Laundering and Terrorist Financing Prevention Act

Summary

Background

Dutch policy to prevent and combat money laundering is based on the recommendations of the Financial Action Task Force (FATF) and EU directives and regulations. The FATF - an intergovernmental body set up by the G7 in 1989 - focuses on global prevention of money laundering, terrorist financing and other related threats to the integrity of the international financial system. Members of the FATF, including the Netherlands, have committed themselves to implement the forty FATF recommendations to prevent and combat money laundering, terrorist financing and the financing of proliferation and to implement measures to improve national legal and regulatory systems and international cooperation in this field. The majority of the FATF's recommendations has been adopted into the fourth EU Anti-Money Laundering Directive, applicable to all EU member states. In short, Article 7 of this directive obliges EU member states to implement a risk-based policy against money laundering and terrorist financing and to establish a *National Risk Assessment (NRA).*

The Ministry of Finance and the Ministry of Security and Justice[1] have commissioned the Research and Documentation Centre (WODC) to carry out the first NRA. The goal of this NRA is to identify the ten greatest risks relating to money laundering in terms of their potential impact and to assess the 'resilience' of the policy instruments designed to prevent and combat money laundering. Resilience entails the functioning of policy instruments (including legislation), whereby the following is applicable: the greater the resilience, the more the risks are combatted. This initial NRA also describes a number of lessons learned that could be taken into account in the process of subsequent NRAs.

The WODC also conducted a NRA on terrorist financing at the same time as this NRA. For this purpose, the same research methodology was used and largely the same expert organisations were consulted.

What is money laundering?

Money laundering can be defined in both legal and economic terms. From a legal perspective, money laundering is when somebody hides or conceals the true nature, origin, place where it was found, disposal or relocation of an object; or hides or conceals who the legal owner is or who is in possession of the object; despite knowing that or being in a position in which they should reasonably suspect that the object in question was either directly or indirectly obtained as a result of any crime. From an economic perspective, the process focuses on how money obtained from criminal activity is introduced into the legal financial system with a view to conceal the criminal origin of the money. In general, the process of money laundering can be divided into three stages:

- Placement: criminal funds are introduced into the financial system.
- Concealment: the origin of the criminal funds is concealed.

[1]Since the Rutte III cabinet took office, on 26 October 2017, the Ministry of Security and Justice has been renamed Ministry of Justice and Security. Because the NRA was completed before the installation of the new cabinet, we refer to this ministry with the old name.

- Integration: the criminal funds are invested in legal projects, objects or goods.

Money laundering is always preceded by some form of crime, such as drug trafficking, human trafficking, theft or social/tax fraud. Different channels are used to launder the proceeds of crime, such as banks, providers of payment services and real estate. Within these channels, different methods are applied that are connected to the aforementioned money laundering stages.

Research methodology

The research methodology used for this initial NRA is qualitative in nature and predominantly based on experts' opinions and estimates. In short, the research methodology involves the following:

- A context analysis that depicts specific circumstances in the Netherlands that are believed to be of influence in regard to the prevalence of money laundering. For the purposes of this context analysis, a literature study was conducted.
- In order to identify threats relating to money laundering, the following activities were conducted:
  - An extensive literature study (examining six foreign NRAs, the European Supranational Risk Assessment, the National Threat Assessment for Organised Crime 2017-2021 and other relevant reports).
  - An e-mail questionnaire was sent to representatives of supervisory, investigative and law enforcement authorities in the area of money laundering, as well as umbrella or sector organisations of entities that are obliged to report unusual transactions. In this report, such organisations are referred to as 'expert organisations'[2].
  - Interviews were held with academics and representatives of expert organisations.
- An initial expert meeting was conducted in which representatives of expert organisations identified the money laundering risks which they perceive as having the greatest potential impact. They also estimated the potential impact of these risks.
- After the expert meeting, an e-mail questionnaire was sent to the participants to inquire which data reflect the prevalence of the ten identified risks. In the questionnaire, the experts were also asked if these data were available to third parties and which other – now unavailable – data exist that reflect the prevalence of the ten identified risks.
- In a second expert meeting, representatives of expert organisations assessed the resilience of the available policy instruments designed to prevent or combat the ten risks.
- In the final stage of the research, a series of validation interviews were conducted with key experts with the primary purpose of examining to what extent they recognise the identified risks and whether any significant risks have been overlooked.

[2] These include a substantial number of organisations such as the Public Prosecution Service, the National Police, the Financial Intelligence Unit - the Netherlands, The Dutch Central Bank and the Dutch Authority for the Financial Markets.

What makes the Netherlands vulnerable to money laundering?

According to various studies, the Netherlands is vulnerable to money laundering due to its open, commerce-oriented economy, its vast and internationally oriented financial sector and the scale of criminal income from fraud (including tax fraud) and drug-related crime. These are the conclusions issued by the FATF in its Mutual Evaluation Report of the Netherlands of 2011. These results were confirmed by research and publications by other institutes, including publications recently released in 2017. In addition, the results of the Transcrime project IARM[3] show that the Dutch gambling, catering, and art and entertainment sectors are vulnerable to money laundering due to the involvement of organised crime, the occurrence of fraudulent activity, the widespread use of cash in these sectors and lack of clarity regarding ultimate beneficial owners. This latter aspect was also mentioned in a recent report by Transparency International Netherlands, in which the Netherlands is considered lagging behind with regard to the central registration of ultimate beneficial owners.

However, the Netherlands also has characteristics that make it less vulnerable to money laundering in comparison to other countries. For example, the extent of organised crime in the Netherlands is relatively small and there are very few black markets for smuggled goods.

Risks relating to money laundering

The representatives of expert organisations selected ten greatest risks in terms of potential impact from a longlist of threats related to money laundering. This longlist has been whittled down by experts using a two-step process resulting in the ten risks in terms of the greatest significant potential impact. They then estimated the potential impact of these risks over two rounds by means of a multi-criteria analysis.

Table S.1 The ten main money-laundering-related risks according to the experts

Risk	Potential risk level (scale from 0-100)
Money laundering via financial institutions (especially banks)	71-75
Money laundering via payment service providers	61-70
Money laundering via trust offices	
Money laundering via offshore firms	
Money laundering constructions to conceal actual value	55-60
Trade-Based Money Laundering	
Money laundering via fiscally driven/complex corporate structures	
Money laundering via virtual currencies	
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	
Money laundering via national and international investment structures for value transfer	

[3] The full name of the Transcrime project is: “Identifying and Assessing the Risk of Money Laundering in Europe”.

The estimated potential impact of the ten greatest risks related to money laundering are displayed as a range (see Table S.1). A range was used as the maximum and the minimum risk levels of the risks were not substantially far apart, a number of risk levels were relatively close to one another and not all estimates by the experts were or could be entirely substantiated. Money laundering via financial institutions was assessed as having the highest potential impact. Experts attributed the highest potential risk level to bank services since they risk being abused due to the vast amounts of money involved in their operations.

During the expert meeting, the attention focused on money laundering risks that the participants believe to exist *at this current moment*. During both the expert meeting and the in-depth interviews, only limited information was obtained regarding possible 'future risks'. One possible future risk that was mentioned relates to the 'new economy', reflecting global technological changes in fields as telecom and the internet. The introduction of new technologies, products and services creates new opportunities for criminals to launder their illicit income. One of the ten risks identified during the expert meetings - money laundering via virtual currencies - is 'future-oriented' in nature. As the experts have as yet barely encountered this risk in their everyday professional practice, the substantiation of this risk leaves something to be desired. At the same time it was considered that despite the considerable fluctuations in value of several virtual currency denominations such as bitcoin, ethereum and monero in the last year, the overall trend is a vast and steady value increase of 'crypto currencies'. Virtual currencies were identified as a possible future risk mainly because of the attention generated by this sharp increase in value and the (as yet) limited resilience of the instruments to mitigate the risks.

Resilience of policy instruments

The available policy instruments targeting the prevention and/or combat of money laundering include the relevant instruments stemming from local, national and international legislation, sector-oriented regulations, and regulations within organisations. The intention of this NRA was not to create a complete list of these policy instruments: the research focused on the policy instruments mentioned by the representatives of the expert organisations during the second expert meeting.

With regard to national legislation, the *Money Laundering and Terrorist Financing Prevention Ac*t is an important instrument in preventing money laundering. The Act imposes a number of obligations on financial institutions and designated non-financial businesses and professions (the DNFBPs) such as obligations to undertake costumer due diligence measures (obligatory identification of the client and the ultimate beneficial owner) that need to be enhanced if there are higher risks of money laundering, and to report unusual transactions of clients to the Financial Intelligence Unit –the Netherlands. Other national laws and regulations relevant for combating money laundering include the *Financial Supervision Act* (regulating the financial sector in the Netherlands), the *Dutch Penal Code*, the *Trust and Company Service Providers (Supervision) Act* (regulating the integrity of trust offices), *Dutch tax law*, the *Public Administration Probity Screening Act* (Wet Bibob) and the *Commercial Register Act 2007*.

There is also specific European legislation to combat money laundering. Primarily, there is the fourth *EU Anti-Money Laundering Directive*, which is currently being transposed into national law. There is also the *EC Regulation on controls of cash*

entering or leaving the Community, which obliges all natural persons who enter or leave the EU in possession of EUR 10,000 or more in cash to report this to the authorities. Furthermore, the revised *Wire Transfer Regulation* obliges all payment service providers and intermediary payment service providers to record information not only about the sender, but also the recipient.

The sector also has a number of self-regulatory measures to prevent and combat money laundering, such as the general banking terms and conditions that describe the rules of conduct between banks and their clients. Furthermore, banks affiliated with the Dutch Banking Association and the Dutch Finance Houses' Association can record the names of clients who committed money laundering in their collective fraud-prevention system (the *External Referral Application*).

The experts who were consulted during this study indicated that in principle, they are positive about the instruments at their disposal. According to them no important elements are missing. However, this does not mean that they believe the available policy instruments can entirely eliminate the risks relating to money laundering. During a second expert meeting, the experts were invited to consider to what degree the identified risks would be eliminated by the application of the policy instruments. They estimated that the instruments would reduce the money laundering risks identified in this NRA on average by around one-third (see Table S.2).

Table S.2 Average resilience of the entire range of policy instruments per risk

Risk	Type of risk	Resilience (on a scale of 0-100%)
Money laundering via financial institutions (especially banks)	Money-laundering channel	41-50%
Money laundering via payment service providers	Money-laundering channel	
Money laundering via trust offices	Money-laundering channel	31-40%
Money laundering via fiscally driven/complex corporate structures	Money-laundering method	
Money laundering via national and international investment structures for value transfer	Money-laundering method	
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	Money-laundering method	21-30%
Money laundering constructions to conceal actual value	Money-laundering method	
Money laundering via offshore firms	Money-laundering method	
Trade-Based Money Laundering	Money-laundering method	
Money laundering via virtual currencies	Money-laundering method	11-20%
Average resilience		32%

The resilience of the policy instruments is relatively highest for the risk of 'money laundering via financial institutions (especially banks)' and 'money laundering via payment service providers' since these sectors are regulated, and (prohibited) anonymous transactions, according to experts, are addressed effectively in the Netherlands. At the same time the experts noted that the available policy instruments to prevent and/or combat money laundering have its limitations in an international environment, for example in trade-based money laundering and money laundering via offshore firms. For the combat of money laundering in an international/cross border context international collaboration and data sharing between supervisory, investigative and enforcement bodies is key. However, such

international collaboration appears difficult to realise in practice because of different definitions of money laundering and different judicial systems. The experts also believe the available policy instruments are insufficient to effectively mitigate money laundering risks involving unlicensed financial institutions and service providers, for example, unlicensed payment service providers or underground banking. Furthermore, there is a relatively low level of resilience against unregulated methods allowing anonymous transactions, such as money laundering via virtual currencies and underground banking. The nature and methodology of virtual currencies is still evolving, hence, the risks have not yet been fully crystallised. For this type of risk, the experts believe that the existing policy instruments offer only limited resilience.

In conclusion

The initial NRA gave insight in the ten risks that experts believe to have the greatest potential impact and in the resilience of the policy instruments available for the prevention and/or combat of money laundering. As mentioned earlier, the research methodology used for this initial NRA is qualitative in nature and is predominantly based on experts' opinions and estimates. During subsequent NRAs, efforts could be made to ensure the research methodology is more data-oriented, as this will reduce dependency on possibly subjective expert opinions and mitigate the risks involved in this. Quantitative data could be incorporated into expert meetings as much as possible in order to help ‘synchronise’ the experts' frames of reference. Also, the longlist of threats should –to the greatest extent possible –be based on available data that indicate the prevalence and potential impact of these threats. Finally, greater substantiation could be given for the identification of the ten risks, preferably backed up with data.

During the expert meetings for this first NRA, there was not sufficient time to substantiate all expert opinions or to elaborate case studies. As a result, certain parts of this NRA are more general in nature. In the next NRA, attention could be paid to deepen the insight in the risks relating to money laundering and the resilience of the policy instruments.

1 Introduction

1.1 Background

Dutch policy to prevent and combat money laundering is based on the recommendations of the Financial Action Task Force (FATF)[4] and EU directives and regulations. The FATF – an intergovernmental body established by the G7 in 1989 – focuses on global prevention of money laundering, terrorist financing and other related threats to the integrity of the international financial system. Members of the FATF, including the Netherlands, have committed themselves to implement the forty FATF recommendations to prevent and combat money laundering, terrorist financing and the financing of proliferation and to implement measures to improve national legal and regulatory systems and international cooperation in this field.[5] The majority of the FATF's recommendations has been adopted into the fourth EU Anti-Money Laundering Directive, applicable to all EU member states.[6] In short, Article 7 of this directive obliges EU member states to implement a risk-based policy against money laundering and terrorist financing, and to establish a National Risk Assessment (NRA).

In 2016, the Research and Documentation Centre (WODC, part of the Ministry of Security and Justice[7]) conducted an exploratory study on the methods and data to be applied for the first NRA.[8] The study presented a growth model for the Dutch NRA, in which the quality of successive risk assessments will increase by applying the learning gained from previous assessments, and by making each NRA more data-oriented than its predecessor. The present report is the first Dutch NRA.

In parallel the WODC also completed a NRA on terrorist financing.

1.2 What is money laundering?

Money laundering can be defined in both legal and economic terms. [9] The legal perspective on money laundering is based on the Dutch Penal Code (WvS), Articles 420bis, bis.1, ter, quater and quater.1, which describe the circumstances that render a person guilty of money laundering. From a legal perspective, money laundering is when somebody hides or conceals the true nature, origin, place where it was found, disposal or relocation of an object; or hides or conceals who the legal owner is or who is in possession of the object; despite knowing that or being in a position in which they should reasonably suspect that the object in question was either directly or indirectly obtained as a result of any crime. Here, 'object' is

[4] FATF (2012).

[5] www.fatf-gafi.org.

[6] See the bibliography for official titles and sources of legislation.

[7] Since the Rutte III cabinet took office, on 26 October 2017, the Ministry of Security and Justice has been renamed Ministry of Justice and Security. Because the NRA was completed before the installation of the new cabinet, we refer to this ministry with the old name.

[8] Van der Veen & Ferwerda (2016).

[9] Soudijn & Akse (2012).

defined as any good or any property right .[10] From an economic perspective, the process focuses on how money obtained from criminal activity is introduced into the legal financial system with a view to conceal the criminal origin of the money.[11] In general, the process of money laundering can be divided into three stages:[12]

- Placement: criminal funds are introduced into the financial system.
- Concealment: the origin of the criminal funds is concealed.
- Integration: the criminal funds are invested in legal projects, objects or goods.

Money laundering is always preceded by some form of crime, such as drug trafficking, human trafficking, theft or social/tax fraud. Different channels are used to launder the proceeds of crime, for example, through financial institutions, payment service providers and real estate. Within these channels, different methods are applied that are connected to the aforementioned money laundering stages. This NRA focuses primarily on the economic perspective of money laundering.

1.3 Aim and research questions

The objective of this NRA is to identify the ten greatest money-laundering risks, and to assess the 'resilience' of the policy instruments (legislation) designed to prevent and combat money laundering. This initial NRA focuses on analysing the ten risks chosen from a longlist of threats related to money laundering by experts as having the greatest potential impact.

The NRA is structured around the following elements:

- A *context analysis*, that depicts specific circumstances in the Netherlands that are believed to be of influence in regard to the prevalence of money laundering.
- The *risk identification* stage, which involves determining and ranking the ten risks relating to money laundering with the greatest potential impact in the Netherlands, as selected from a longlist of threats; and
- The *risk analysis* stage, which helps to determine the extent to which the available anti-money laundering policy instruments combat the risks identified as having the greatest potential impact.

The NRA offers a response to the following research questions:

1 What context variables make the Netherlands vulnerable to money laundering?
2 Which ten risks relating to money laundering can, in view of the Dutch context, be deemed as having the greatest potential impact?
3 Which risks have not yet been identified in the Netherlands, but could be relevant in the future? How can more insight into this situation be obtained?
4 What policy instruments are available in the Netherlands to combat the risks?
5 To what extent can the existing range of policy instruments be expected to effectively combat the risks?
6 Which risks are not addressed effectively by Dutch policy instruments, and why? What measures could resolve this situation, and to what extent are they feasible?
7 Which risks remain after implementation of the policy instruments? How serious are the remaining risks relative to one another?

---

[10] Dutch Penal Code (WvS), Articles 420bis, bis.1,ter, quater and quarter.1; see the bibliography for official titles and sources of legislation..

[11] Soudijn & Akse (2012, p. 13 et seq.).

[12] Soudijn & Akse (2012, p. 13); www.fatf-gafi.org/pages/faq/moneylaundering/.

To facilitate future NRAs, this initial NRA also answers the following research questions:

1 What quantitative data could be used in subsequent NRAs to identify money-laundering risks?
2 What are the lessons learned that could be applied to subsequent NRAs?

1.4 Limitations of this initial NRA

The methodology used for this initial NRA is in line with the FATF Standards[13] and the recommendations from the exploratory study on methodology and data that was conducted in 2016.[14] The above implies that this initial NRA acknowledges the following limitations:

- The number of risks was limited to the ten risks representing the greatest potential impact, selected from a longlist of threats related to money laundering.
- Because the NRA is based on the opinions of experts in the area of money laundering, the determination of the key risks contains a subjective element and may be subject (at least in part) to individual perceptions or personal opinions.
- The present NRA does not cover the situation on the islands of Bonaire, Sint Eustatius and Saba (the BES-islands).

The NRA growth model means that learning opportunities must be detected and explicitly formulated during each NRA. Transparency on the analyses carried out and their results is crucial in order to make use of these opportunities. Transparency also makes the analyses reproducible, which is an important requirement from an academic/scientific research perspective. The methodological exploratory study revealed that the level of transparency in the analyses of the foreign NRAs was not sufficient to provide reproducibility.[15]

1.5 Document overview

Section 2 focuses on the research methodology that was applied to this initial NRA on money laundering, and explains the key concepts used throughout the NRA and this report. Section 3 describes the conditions that render the Netherlands susceptible to money laundering, as revealed in previous research, and substantiates this on the basis of some geographic, demographic, economic and criminological characteristics of the Netherlands that can help facilitate money laundering. As money laundering is always preceded by crimes revolving around the illegal acquisition of objects, it devotes special attention to trends in the prevalence of proceeds of crime in the Netherlands. Lastly, several characteristics are listed that actually help discourage money laundering in the Netherlands.
Section 4 firstly presents the longlist of money-laundering threats, which provided the basis for the expert meeting in which the experts identified the ten risks they perceived as having the greatest potential impact. The results of the first expert meeting are then described, and the section concludes with a look at the data that are or are not available on the prevalence of the ten identified risks.
Section 5 looks first of all at the policy instruments available in the Netherlands for preventing and/or combating money laundering, and then presents the experts'

[13] FATF (2013a).

[14] Van der Veen & Ferwerda (2016).

[15] Van der Veen & Ferwerda (2016).

assessments of the resilience of the policy instruments regarding each of the ten identified risks.
Section 6 outlines the key results of the NRA by answering the research questions. This is followed by an evaluation of the NRA, highlighting both the strengths and areas for improvement of the research methodology applied. Finally, this section discusses some lessons learned that may be useful in designing the next NRA.

2 Research methodology

This section outlines the approach taken to this initial NRA on money laundering. Firstly, the key NRA concepts are introduced and defined. The research plan, process and the methods applied are described in terms of the three stages of the NRA, i.e. context analysis, risk identification and risk analysis. These stages are part of the ISO 31000 risk-management method,[16] which was taken as the core framework for this NRA.

2.1 Key NRA concepts

The NRA focuses on the following key concepts: threats, consequences, vulnerabilities, risks and resilience. The FATF Guidance supporting the NRA process, offers the following definitions for the first four of these concepts:[17]

- *Threats* are persons or groups of people, objects or activities with the potential to cause harm to, for example, the state, the society and the economy. In the context of money laundering this includes criminals, their deliberate or unwitting facilitators, their intended or completed transactions, and the money-laundering activities they develop.
- *Vulnerabilities* compromise those things that can be 'exploited' by the threats (i.e. people, groups of people, objects or activities that are potentially harmful to the state, society, or the economy). These may include weaknesses in the system that provide opportunities for money laundering, or the specific features/characteristics of a country, sector, service or financial product that make it susceptible to harm or other consequences of a threat.
- *Consequences* refer to the effects resulting from money laundering, also known as the 'impact'. These can include the effects of criminal activities on the financial system, financial institutions, the economy or society. These consequences are not only adverse in nature: criminals also spend some or all of their income in the regular economy, which can also have a positive impact.
- The *risks* of money laundering are a function of the three above-mentioned factors (threats, vulnerabilities and consequences), which leads to the following risk function: $r=f(t,v,c)$.[18]

As shown above, the FATF risk function includes the element of vulnerability. This NRA defines this element as:

- the geographic, demographic, or economic context factors that may be of influence in regard to the prevalence of money laundering in the Netherlands; and
- the Dutch criminal landscape aimed at generating income (including property and drug-related crime), which can precede to money laundering . The context analysis provides an overview of the types of crime that can precede money laundering in the Netherlands, which are aimed at acquisition of objects/assets.

In addition to the vulnerabilities, this initial Dutch NRA also considers factors that may serve to limit – or even eradicate – the potential for harmful activity. These may include accurate registrations, supervision, sufficient enforcement and

[16] Risk management according to the standards of the International Organization for Standardization.

[17] FATF (2013a).

[18] Where r = risk, t = threat, v = vulnerability and c = consequence.

detection capacity, quality, and professionalism. These factors fall under the element of resilience:

- *Resilience* concerns the effectiveness (including both the intended purpose and implementation) of the policy instruments available in the Netherlands for preventing or combating money laundering and the various associated risks whereby the following is applicable: the greater the resilience, the more the risks are combatted. The Irish NRA also added an element to the FATF methodology, indicating the extent to which the threats were mitigated by policy measures, known as the 'mitigants'.[19]

'Resilience' was added to the FATF methodology as it provides concrete starting points for the formulation of new policy or the enhancement of existing policy aimed at combating the money-laundering risks identified by the NRA, i.e. those with the greatest potential impact.

The precise distinction drawn in the NRA between 'threats' and 'risks' requires some clarification, which is provided by the research methods applied. The following section looks at this aspect in greater detail. A literature study, an e-mail questionnaire among representatives of 'expert organisations'[20] and interviews with academics were employed in order to generate a longlist of money-laundering threats. A 'threat' differs from a 'risk' in the sense that the associated vulnerabilities and potential impact (the *consequences*) have not (or not yet) entered into the picture.

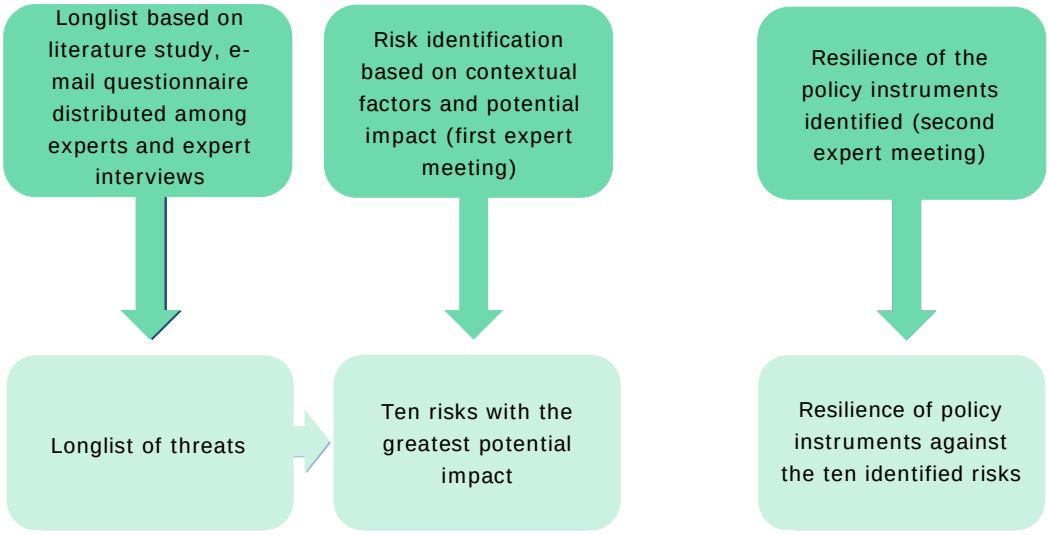
During the first expert meeting, the threats were presented alongside the vulnerabilities and the threats' potential consequences/impact. The experts present were first required to select from a longlist the ten threats that they believed posed the greatest potential impact, including a consideration of the existing vulnerabilities and their own estimation of the potential impact. From that point on, the threats were referred to as 'risks'. The potential impact was then estimated in greater detail by experts, based on a Multi-Criteria Analysis (MCA).

During the second expert meeting, the resilience of the existing policy instruments for preventing and combating the identified risks, was incorporated into the analysis, allowing the meeting to determine the degree to which the risk would be eliminated by application of the available instruments. A diagram of this process is given in figure 2.1.

[19] Department of Finance & Department of Justice and Equality (2016).

[20] Here, 'expert organisations' are defined as supervisory, investigative and law enforcement authorities in the area of money laundering, as well as umbrella or sector organisations of entities that are obliged on the basis of the Money Laundering and Terrorist Financing Prevention Act (Wwft) to report unusual transactions. Hereinafter such organisations are referred to as 'expert organisations'.

Figure 2.1 Dutch NRA Method



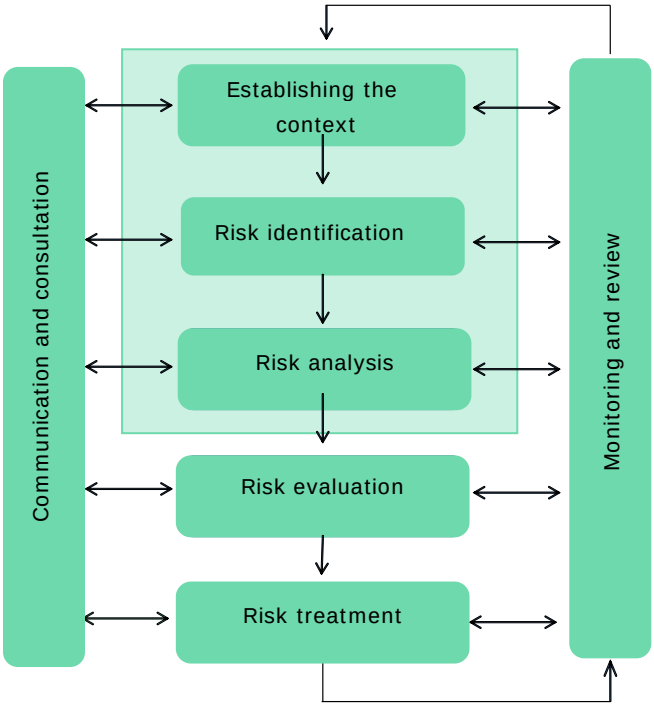
2.2 The ISO 31000 framework

The NRA was conducted within the ISO 31000 risk management framework: a set of international standards allowing the application of a wide variety of methods. The FATF Guidance also follows this overall structure.[21] The present NRA does not cover the full risk-management cycle as described by ISO 31000 – it is limited to the context analysis, risk identification and risk analysis. The exploratory study conducted in 2016 already attested to the fact that the NRA was conducted according to scientific research principles.[22] Risk evaluation and treatment involve making decisions on the extent to which risks are deemed acceptable or tolerable, and whether new or amended policy is necessary. Because normative decisions of this type are at odds with the scientific research approach of the NRA, risk evaluation and risk treatment fall outside the scope of this NRA.

[21] FATF (2013b).

[22] Van der Veen & Ferwerda (2016).

Figure 2.2 The risk-management process based on the ISO 31000 framework (focus of the NRA in light-green)



2.3 Methods applied

Each component of ISO 31000 allows for the application of specific research methods. The exploratory study from 2016 revealed the following most suitable methods for the first NRA: checklists, brainstorming, an MCA (see Box 2.2) and the Delphi method (see Box 2.3).[23] The present NRA is based on these predominantly qualitative methods.

Initially, written sources were consulted. In addition to academic sources and statistics, these also included the NRAs of other countries and the European Supranational Risk Assessment (SNRA),[24] the National Threat Assessment for Organised Crime 2017-2021 (NDB), parliamentary records and guidelines, and other sources from the European Commission and the FATF.
The bulk of the information for the NRA was obtained from an independent collection of data among academics, representatives of expert organisations and policy officers at the Ministries of Finance and Security & Justice, via interviews, e-mail questionnaires and expert meetings. The risks were ultimately identified during

[23] Van der Veen & Ferwerda (2016).

[24] European Union Fourth Anti-Money Laundering Directive, Article 6, which states: 'The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate [paragraph 1]. The report referred to in paragraph 1 shall cover at least the following: (a) the areas of the internal market that are at greatest risk; (b) the risks associated with each relevant sector; (c) the most widespread means used by criminals by which to launder illicit proceeds [paragraph 2]'; see the bibliography for the official titles and sources of legislation.

expert meetings attended by representatives from expert organisations, the aim of which was to collate all relevant perspectives on preventing and combating money laundering.[25]
The expert meetings were structured using a Group Decision Room (GDR), which is characterised by an alternation between the use of ICT and group discussions (see Box 2.1). The running sheets that were drawn up for the expert meetings helped to structure the sessions and avoid running overtime.[26] The experts were given as much opportunity as possible within the given time constraints to explain, substantiate and discuss their judgements, as well as question one another about them.
A well-known pitfall of GDR is that of 'group thinking', which was avoided through the appointment of a professional, independent chairperson whose task was to encourage the experts to substantiate and explain the judgements they had submitted to the GDR environment, and to present case studies. The expert meetings were run by APE Public Economics, which also supplied the chairperson and reported the expert meetings.[27]

Box 2.1 Group Decision Room (GDR)

A GDR is an electronic conference system that allows the participants to produce a large amount of ideas and opinions in a short period of time by alternating between IT methods and plenary discussions. For these reasons, group discussion rooms are also referred to as 'acceleration rooms'. In the GDR, all participants have a device (tablet or laptop) that allows them to ask and answer questions, provide input and vote digitally on statements. The answers and responses by all participants are collated and stored centrally.

The GDR environment provides aggregated overviews in real time, showing the degree of consensus among the participants. These overviews are projected centrally, and serve as input for group discussions that allow for qualitative enhancement and substantiation of the results. The purpose of GDRs is to save time and to broaden the support base for the results of the meeting. GDRs facilitate transparency in meeting outcomes.

A NRA on terrorist financing was also conducted parallel to this NRA on money laundering, which applied the same research methodology. In many cases (but not all) the same representatives of expert organisations were interviewed and attended the expert meetings. The Anti Money Laundering Centre (AMLC) was involved in the research for the NRA on money laundering, which was not the case for the NRA on terrorist financing. Conversely, the Fiscal Intelligence and Investigation Service (FIOD) and the General Intelligence and Security Service (AIVD) were involved in the research on terrorist financing, but not money laundering. Lastly, it should be noted that a wide range of literature was used for much of the context analysis (see Section 3).

The sections below explain which methods were used for the various stages of the NRA, and why.

[25] A list of the expert organisations represented at these meetings is given in Appendix 3.

[26] The running sheets used are given in Appendix 4.

[27] Technical GDR services were provided by Spilter, whose employees supplied technical support during the expert meetings.

2.4 Stage 1: Context analysis

First of all a literature study was conducted, focusing on the context factors relevant to money laundering and the prevalence of financial or property crime. An overview was created of the various forms of crime in this area as identified by Statistics Netherlands (CBS). The factors involved are those that may correlate to the prevalence of money laundering in the Netherlands.

The purpose of the context analysis was to establish a reference framework for the experts, to ensure that their judgements on the potential impact of money-laundering threats were all based as much as possible on the same basic information regarding the Dutch context in which it takes place.

2.5 Stage 2: Risk identification

The risk identification stage involved determining which ten risks relating to money laundering have the greatest potential impact in the Netherlands. The risks were selected by experts from a longlist of money-laundering threats, based on the findings of the research activities described below.

2.5.1 Longlist of threats

Analysis of relevant documents
The first step involved analysing the results from the six foreign NRAs, the European SNRA, the NDB and other relevant reports, to generate a list of relevant money-laundering channels and methods, and their associated predicate crime.[28]

E-mail questionnaire among representatives of expert organisations
Secondly, a brief e-mail questionnaire was distributed among representatives of expert organisations in the field of money laundering. A total of 32 organisations were approached, 16 of which completed the questionnaire. The respondents included five supervisory bodies, the Financial Intelligence Unit Netherlands (FIU Netherlands), the Public Prosecution Service (OM), the National Police, the Anti-Money Laundering Centre (AMLC), Customs Netherlands (*Douane Nederland*), the The Hague Bar Association /Money Laundering and Terrorist Financing Prevention Act Information Service (*Kenniscentrum Wwft*) and five sector/umbrella organisations of obliged entities.

In the questionnaire the experts were asked to identity the ten main money-laundering related threats in the Netherlands. Their responses were collated into a longlist of threats at various levels, which included money-laundering channels and methods and the associated predicate forms of crime. The questionnaire also asked which criteria the organisations deemed important when weighing up and prioritising the threats.

In-depth interviews
The final step in the research stage involved face-to-face interviews on money laundering: four with academics, and eleven with a total of 24 representatives from

[28] See the bibliography for a list of the literature consulted.

expert organisations in the field of money laundering.[29] The following expert organisations were represented:

- five supervisory bodies: Netherlands Authority for the Financial Markets (AFM), the Financial Supervision Office (BFT), the *Wwft* Supervision Office (BTW), the Dutch Central Bank (DNB) and the Netherlands Gaming Authority (KSA);
- AMLC;
- Customs Netherlands (*Douane Nederland*);
- FIU Netherlands;
- The Hague Bar Association /Money Laundering and Terrorist Financing Prevention Act Information Service (*Kenniscentrum Wwft*);
- the National Police;
- the Dutch Banking Association (NVB);
- the Public Prosecution Service (OM).

One outcome from these interviews was an improved understanding of exactly how certain threats (some of which had already been reported in the questionnaire) can or do manifest. The interviews also provided an initial overview of the existing available policy instruments, and their effectiveness.

Focus on laundering channels and methods

Some of the foreign NRAs consulted were structured around the types of crime that precede money laundering. Rather than these predicate offences, the Dutch NRA focuses on the channels and methods used to launder money, for the following reasons:

- Focusing on channels and methods - rather than on the predicate offences - reveals the different ways in which money laundering manifests in practice. This provides concrete starting points for generating new policy or enhancing existing policy to combat money laundering.
- The longlist of threats is predominantly based on the threats identified by the expert representatives themselves in the e-mail questionnaire and the interviews: they primarily saw money-laundering channels and methods as threats, rather than the predicate offences.

2.5.2 First expert meeting

The aim of the first expert meeting was to condense the longlist of the ten risks with the greatest potential impact. The meeting was attended by sixteen representatives from expert organisations:[30]

- five supervisory bodies: AFM, BFT, BTW, DNB and the Netherlands Bar Association (NOvA);
- six sector/umbrella organisations: Holland Quaestor (trust offices), Royal Dutch Association of Civil law Notaries (KNB), the Netherlands Institute of Chartered Accountants (NBA), the Dutch Banking Association (NVB), the Netherlands Association of Brokers and Appraisers (NVM) and the Netherlands Association of Financial Transaction Agencies (NVGTK);
- AMLC, Customs Netherlands, FIU Netherlands, the Royal Netherlands Marechaussee (KMar) and the Public Prosecution Service (OM).[31]

[29] See Appendix 2 for a list of the expert organisations whose representatives were interviewed.

[30] Eighteen representatives were invited in total. See Appendix 3 for a list of the expert organisations represented in the first expert meeting.

The experts were selected by their organisations based on their knowledge of the formation and implementation of Dutch anti-money laundering policy. The participating experts did not necessarily represent the opinions of their respective organisations. They were explicitly asked for their views on the various issues raised during the expert meeting, based on their personal experience with, and wide-ranging expertise on, the prevention and combating of money laundering.
Via the GDR environment, the experts in the meeting were presented with a longlist of thirty money-laundering threats, to which they could add threats. They were then asked to choose the ten threats from the list which, according to them, had the greatest potential impact. Aggregating the submissions produced a ranked list of threats: the ranking was discussed, after which the experts were asked to once again choose the ten threats with the greatest potential impact, based on the preceding discussion. This exercise produced a new ranked list of threats.
In their selections, the experts incorporated the contextual factors affecting the prevalence of money laundering in the Netherlands. They were also asked to consider the 'potential impact' of the threats, without this concept having been defined in advance.[32] After identifying the ten threats with the greatest potential impact, the 'threats' became known as 'risks', and their potential impact specified in greater detail using an MCA.

Box 2.2 Multi-Criteria Analysis (MCA)

MCA is a method used to facilitate the most rational choice possible from a range of potential policy decisions or other decisions. To compare the various alternatives, a set of criteria is determined that enables the options to be evaluated, and may include aspects such as cost, safety, environmental quality, social impact, feasibility and acceptability. Experts or other stakeholders allocate weighting scores to each alternative and assessment criterion, which are then standardised. Next, the scores are added up for each alternative, and the option with the highest score is deemed the most suitable to fulfil the requirements of the specific decision-making scenario at hand.

Take buying a new car, for example: criteria such as the purchase price, fuel consumption and colour can all influence the decision. After a shortlisting process, the two remaining alternatives are a blue Volkswagen and a red Ford. When deciding which one to buy, the important criteria are the purchase price, fuel consumption and colour, and they all affect the decision to a different extent. As part of an MCA, each criterion is weighted (e.g. on a scale of 1-10). For example: the purchase price may be weighted at 8, fuel consumption at 9 and colour at 6. Next, for each car is determined how it scored on the criteria (on a scale of 1-100), producing a table such as the following:

Criterion	Weighting	Volkswagen	Ford
Purchase price	8	60	75
Fuel consumption	9	90	60
Colour	6	80	60

The Volkswagen may cost more than the Ford, however its fuel consumption is much lower and the buyers like the colour better. An MCA helps to order the

[31] An expert representative from the National Police was also invited. Because this person did not attend, a validation interview was conducted with the expert at the conclusion of the field work with the purpose of examining to what extent the expert recognises the ten key risks identified.

[32] Unlike the MCA, in which the potential impact was established using predefined criteria.

available alternatives for decision-making. The resulting impact matrix from the figures above shows that the Volkswagen is the most rational choice.

Criteria	Volkswagen	Ford
Purchase price	48	60
Fuel consumption	81	54
Colour	48	36
Total score	**177**	**150**

An MCA gives both structure and transparency to complex decision-making processes, allowing the MCA method itself to be developed and fine-tuned. If new information becomes available on the elements in the method such as the criteria, the method can be adapted accordingly. One disadvantage of the MCA applied in the NRA is the reliance on expert judgements that are themselves inherently subjective, and are expressed in the scores used for the MCA calculations.

The MCA helped to formalise the participants' considerations during the expert meeting. First of all, the risks that served in the MCA as the potential decision-making alternatives were elaborated. The criteria were then weighted, and subsequently the risks were scored using the criteria. Finally, the scores for each risk were tallied, producing a list of risks ordered according to their potential impact.

The experts in the meeting were asked to use seven criteria to judge the potential impact (and its extent) of these ten risks, for the following three reasons. Firstly, the approach 'objectivises' the experts' judgements, as the potential impact is determined using predetermined criteria, not aspects that can vary between experts. Secondly, it reduces the opportunities for experts to permit their own interests to influence the outcome of the NRA. Thirdly, the approach uses averages, which cover all relevant risk perspectives.
The seven criteria were distilled from the FATF Guidance overview on the consequences of money laundering[33], evaluation of the criteria raised during the expert interviews and a discussion on the criteria by the advisory committee.

The potential impact of the money-laundering risks was determined using the following criteria:
- the stability of the financial system;
- the regular economy;
- society (civil and legal order);
- the degree to which regular society is interwoven with the criminal underworld;
- the manifestation or facilitation of crime or terrorist activities;
- the (perceived) feeling of safety;
- the Netherlands' image/reputation.

During the first expert meeting, the criteria were introduced and the experts were given the opportunity to ask questions about the criteria. They were then asked to weight the criteria, by allocating the relative importance they believe each criterion has when judging the potential impact of the money-laundering risks. The experts did so using a scale from 1-10, where 10 represents the maximum weight.
Next, the experts quantified the extent of the potential impact of each risk on each of the seven criteria.[34] For example, when considering the risk of 'money laundering

[33] FATF (2013, p. 26). The table first appeared in a report by Unger et al. (2006a).

via trust offices' on 'the regular economy', the question to be answered must be read as follows: 'To what extent can money laundering via trust offices affect the regular economy?' The experts could judge the potential impact using a score between 0 and 100, where 0 represents 'no potential impact at all' and 100 represents 'enormous potential impact'. The experts received a handout containing the above-mentioned example, and a scale to assist with making their judgements. They then estimated the relative impact of the risks on each criterion.
When forming their judgements, the experts were asked to disregard the effectiveness of policy aimed at preventing and combating money laundering as much as possible, as this would be the subject of the second expert meeting. Lastly, the average potential impact and the associated spread were determined for each risk, allowing the risks to be ranked according to potential impact. The exact details of the MCA process are given in Box 2.2.

2.5.3 Overview of available data on the identified risks

After the first expert meeting, another brief e-mail questionnaire was send out among the participants. It asked them to indicate what *existing* data provide any information on the current actual prevalence of the ten risks identified during the first meeting, and whether the data is available to third parties. Finally, it asked them what data are still missing that might provide some information on the current prevalence of the ten identified risks. Six of the experts completed the questionnaire, and two replied saying they had trouble answering the questions; the remaining eight did not respond to the questionnaire invitation. Due to both the limited response and the nature of the response, the e-mail questionnaire resulted in little concrete information regarding the availability of data on identified risks.

2.6 Stage 3: Risk analysis

The risk analysis stage aims to provide an understanding of the resilience of the current set of policy instruments aimed at preventing or combating the ten identified money-laundering risks.

2.6.1 Second expert meeting

The purpose of the second meeting was to determine the effectiveness of the available policy instruments in combating the potential impact of the ten key money-laundering risks determined during the first expert meeting. Most of the participants in the second meeting were the same as those who attended the first meeting.[35] Representatives from the fifteen expert organisations below took part.
- Six supervisory bodies: AFM, BFT, BTW, DNB, Ksa and NOvA;
- Five sector/umbrella organisations: KNB, NBA, NVB, NVM and NVGTK;
- AMLC, Customs Netherlands, FIU Netherlands and OM.[36]

---

[34] To ensure a single reference framework for all experts, prior to the meeting they were issued with a summary of the context factors in the Netherlands that can affect the prevalence of money laundering in the Netherlands.

[35] See Appendix 3 for a list of the organisations represented in the second expert meeting.

[36] An expert representative from the National Police was also invited. Because this person did not attend, a validation interview was conducted with the expert at the conclusion of the field work during which the items on the list of the greatest risks identified were discussed.

The experts present were first asked to evaluate the resilience of the current set of policy instruments with regard to the ten identified risks, by describing the degree (i.e. the percentage) to which the potential impact of the risk is combated by the available policy instruments.
Next they identified the policy instruments available in the Netherlands that combat the ten main money-laundering-related risks, from the pool of all relevant instruments stemming from municipal, national and international legislation, sector/industry regulations and measures taken by the relevant organisations themselves. The exercise was not limited to instruments developed specifically for the purpose of preventing and combating money laundering, such as the Money Laundering and Terrorist Financing Prevention Act (Wwft)[37] or the Dutch Penal Code (WvS),[38] but also included policy instruments that combat money laundering as an *additional effect*, such as tax legislation.
The experts were given 100 points to distribute across all policy instruments, where greater effectiveness at preventing or combating money laundering meant a higher score. For example: an expert who believed a policy instrument was crucial in combating money laundering might reserve, say, 80 of their 100 points for that instrument, leaving only 20 points available for allocation to the other relevant policy instruments. Scores were entered in the GDR environment, and the results aggregated, displayed to the group and discussed. When judging the resilience of the policy instruments, the experts made an implicit estimation of their effectiveness. They considered both the theoretical effectiveness of the regulations themselves, as well as the practical effectiveness of the manner of the implementation.
At the end of the expert meeting (following the discussion of the various available instruments and their resilience), the experts were given the opportunity to revise their original judgements, via an (abridged) application of the Delphi method.

Box 2.3 The Delphi method

The Delphi method was developed between 1940 and 1950 (at the start of the Cold War) when, during an American air force project, it became apparent that traditional scientific methods could not provide a satisfactory basis for developing new international warfare techniques. The method involves blending expert judgements when making decisions on matters for which no reliable scientific or academic data exists. The knowledge gaps are filled by the judgements, experiences and intuitions of experts. Revealing these evaluations (in anonymised form) and allowing for more detailed argumentation it enables the experts to revise their initial judgements, which can bolster the consensus regarding a particular solution. The process takes place over a number of rounds.
Benefits of the Delphi method include:
- increased transparency and systematisation of complex decision-making processes;
- enhanced utilisation of existing knowledge and information, as it is shared by experts; and
- increased consensus (in many cases).

The Delphi method was administered via the GDR environment. The discussion of GDR already took account of the potential disadvantages of the Delphi method, i.e. 'group thought'. Experts can sometimes mistakenly believe that they are aware of all relevant facets of a problem. Critical probing by the meeting moderator/chair can

[37] See the bibliography for official titles and sources of legislation.

[38] See the bibliography for official titles and sources of legislation.

mitigate this problem, at least in part.

2.6.2 Validation interviews

At the end of this study, the provisional findings were shared and discussed with representatives of the Ministry of Finance and the Ministry of Security and Justice, as well as representatives of AMLC and the National Police.[39] During the interviews, the items on the list containing the ten risks with the greatest potential impact were discussed; the experts were asked whether they recognise the identified risks and whether any significant risks had been overlooked.

[39] Appendix 2 offers an overview of the interviewed organisations.

3 What makes the Netherlands vulnerable to money laundering?

The first step in the ISO 31000 risk-management system is a context analysis. The analysis presented in this section was conducted using the money-laundering risk factors in the Netherlands named in other studies. It therefore has a different structure and approach than traditional and complete context analyses, such as those created according to the PESTLE method.[40,41] This section begins with a brief description of these studies and their risk factors, which are discussed in greater detail further on. The section concludes with some characteristics of the Netherlands that make it less vulnerable to money laundering.

3.1 Money-laundering risks in the Netherlands: Prior studies

The 2011 FATF *Mutual Evaluation Report* concluded that the Netherlands is vulnerable to money laundering due to its substantial financial sector, its open, commerce-oriented economy, and the scale of criminal income from fraud (including tax fraud) and drug-related crime. [42]

In 2013, Utrecht University completed the ECOLEF[43] study on the effectiveness of anti-money laundering policy in the (then) 27 EU member states,[44] which looked at the money-laundering risks and performance of the policy in each EU country. Like the FATF study, it concluded that fraud, drug trafficking and other drug-related crimes represent by far the greatest proportion of criminal income. The study estimated Dutch criminal proceeds at 14 billion US dollars, or 1.8% of Gross Domestic Product (GDP). The experts consulted also estimated that 'a significant amount of criminal proceeds originating from foreign countries' is laundered in the Netherlands.[45] The ECOLEF study also investigated the money-laundering risk in the (then) 27 EU member states. Defining the level of the threat by the amounts of money to be laundered puts the Netherlands at fifth place within the EU. Expressing the threat as a percentage of GDP drastically alters the outcome, however, and ranks the Netherlands seventeenth among the 27 EU countries (at 14% of GDP).[46]

The CIA World Factbook lists the Netherlands as a significant producer of cannabis and synthetic drugs, including ecstasy.[47] The CIA also sees the Netherlands as a

[40] PESTLE stands for Political, Economic, Social, Technological, Legal and Environmental: these are the elements used in the PESTLE analysis to describe a country, region, business or other organisation. A brief context analysis was conducted for the present NRA; for subsequent NRAs, a more detailed analysis (e.g. one using the PESTLE method) may be used.

[41] Six NRAs from other countries were analysed prior to the creation of this NRA. Only the Irish NRA included a (rather compact) context analysis that included a focus on economic, geographic, political and environmental variables affecting the prevalence of money laundering.

[42] FATF (2011).

[43] This acronym stands for 'Economic and Legal Effectiveness of Anti Money Laundering and Combating Terrorist Financing Policy'.

[44] Unger et al. (2013).

[45] Unger et al. (2013, p. 35).

[46] Unger et al. (2013, p. 39).

[47] Central Intelligence Agency (2017).

gateway into Europe for heroin, cocaine and hash, as well as an important source of the ecstasy that is sold on the US market. The CIA also sees the Netherlands as a great consumer of ecstasy. The International Narcotics Control Strategy Report (INCSR) released by the US Department of State also lists the Netherlands as a transit country for cocaine and as a manufacturer of synthetic drugs (especially ecstasy), most of which is produced for export purposes.[48] The CIA also believes the Netherlands is vulnerable to money laundering due to its substantial financial sector.[49] The INSCR points out that the combination of the Netherlands' open economy and its substantial and internationally oriented financial sector puts it at risk of money laundering; in concrete terms, this relates to financial fraud and tax evasion. Transparency International Netherlands adds that the Netherlands is still lagging behind with regard to the central registration of the Ultimate Beneficial Owner (UBO).[50]

In early 2017, the report by the IARM[51] Transcrime project was released, which investigated the money-laundering risks present in the Netherlands, Italy and the United Kingdom.[52] It employed a new quantitative method for assessing money-laundering risks, and identified the gambling sector as the one presenting the greatest risk in the Netherlands due to the links with organised crime, the prevalence of fraudulent activities, the frequent use of cash and lack of clarity on the ultimate beneficial owners (UBOs). Significant risks were also identified in the hotel and catering industry (hotels and bars in particular have links with organised crime) and the arts and entertainment sector. One of the main aims of the IARM project was to develop an objective and robust method that could serve as an alternative to the predominantly qualitative methods that had been used in NRAs until that time. However, the IARM method has limited application due to the risks being identified in a general, sector-wide context, rather than the specific money-laundering methods used within those sectors. The report therefore concludes that the method requires further development, and argues for the availability of higher-quality data.

3.2 Characteristics of the Netherlands

Before embarking on the money-laundering factors mentioned in the previous study, this section will first look at several fundamental aspects of the Netherlands' geography, population and economy.

3.2.1 Geography and population

Located in north-western Europe, the Netherlands is one of the 28 member states of the European Union (EU). With a population of more than 17 million[53] and a density of over 500 people/km^2, it is the second-most densely populated country in the EU

[48] Department of State (2017a). This US department publishes the INCSR annually, which is divided into two parts. Part 1 deals with the efforts made by the 88 'key countries' to combat drug trafficking (Department of State, 2017a), of which the Netherlands is one. Part 2 describes the measures taken to combat money laundering and financial crime by these countries (Department of State, 2017b).

[49] CIA (2017).

[50] Streiff & Scheltema Beduin (2017).

[51] IARM stands for Identifying and Assessing the Risk of Money laundering in Europe.

[52] Savona & Riccardi (2017).

[53] Statistics Netherlands (CBS) Statline (2017).

(after Malta).[54] Since 2010, the Caribbean islands of Bonaire, Saint Eustatius and Saba (the 'BES' islands) with a total population of around 25,000 have formed part of the Netherlands as 'special municipalities'.[55] The BES islands are also known as the 'Caribbean Netherlands'. Until 2010 they were part of the Dutch Antilles, a former country within the Kingdom of the Netherlands. Besides the Netherlands itself, the Kingdom of the Netherlands also includes Aruba, Curacao and Saint Martin.

3.2.2 Economy

General

The Netherlands' GDP per capita was USD 51,285 in 2016, one of the world's highest according to the OECD.[56] In 2017 the Netherlands was ranked fourth in the Global Competitiveness Report by the World Economic Forum (WEF), superseded only by Switzerland, Singapore and the US. The reasons for the WEF's ranking include the Netherlands' world-class infrastructure, high-quality health care, outstanding higher education system and constant focus on innovation.[57] Other strong economic sectors in the Netherlands include the chemical, logistics and horticultural sectors.[58] The Port of Rotterdam and Amsterdam Airport Schiphol make the Netherlands an important European transport hub.

The financial sector

The Netherlands has a relatively vast and internationally-oriented financial sector, with assets totalling nearly eight times the GDP (770%) in Q1 of 2016.[59] The banking sector represents around half of the financial sector's assets, concentrated in three major banks (ING, Rabobank and ABN AMRO). The combined balance sheet of all three banks totalled €2,066 billion in 2016. ING is the largest bank with a total balance of €845 billion, followed by Rabobank (€663 billion) and ABN AMRO (€394 billion).[60] The Dutch banks' assets are worth nearly four times (385%) the GDP, making the Dutch banking sector one of the largest in the world in relative terms.[61] Insurers represent the smallest of the Dutch financial sectors, with assets at 75% of the GDP. In relative terms, the Dutch pension system is the largest in the world, with assets totalling nearly 200% of the GDP in Q1 2016. Lastly, the relative scope of Dutch investment funds equalled 113% of GDP in Q1 2016.[62]

---

[54] www.volksgezondheidenzorg.info/onderwerp/bevolking/regionaal-internationaal/internationaal#node-bevolkingsomvang-eu-landen.

[55] The BES islands are not included in this NRA, but form the subject of their own separate NRA.

[56] https://data.oecd.org/gdp/gross-domestic-product-gdp.htm.

[57] World Economic Forum (2017); www.weforum.org/reports/the-global-competitiveness-report-2017-2018.

[58] www.topsectoren.nl/topsectoren.

[59] International Monetary Fund (2017, p. 39).

[60] www.banken.nl/nieuws/20396/Ranglijst-grootste-Nederlandse-banken. Consulted on 13 September 2017.

[61] www.banken.nl.

[62] International Monetary Fund (2017, p. 39).

Table 3.1 Scope of the Dutch financial sector (Q1 2016)

Sector	No. of institutions	Assets (in billions of euros)	% total assets	% GDP
Banks	97	€2,605	50%	385
Insurers	190	€505	10%	75
Pension funds	304	€1,330	26%	197
Investment funds	1,832	€767	15%	113
Total	**2,423**	**€5,207**	**100%**	**770**

Source: IMF (2017, p. 39)

The IMF report from which the above data were taken[63] does not address one particular aspect of the Dutch financial sector: the trust sector. This sector is relatively large, consisting of 224 trust offices[64] that manage three-quarters of the roughly 12,000 special financial institutions registered who according to Transparency International operate in the Netherlands.[65, 66] Trust and Company Service Providers (TCSPs) provide a range of services, include being a director of a legal entity or partnership, or providing a postal address in combination with certain administrative services. TCSPs can also use, for the benefit of the customer, a company belonging to the same group (a 'conduit company') for the capital and income from clients' international business operations. It can sometimes be more effective for companies with international operations to have a Dutch legal or corporate entity managed by a trust office. Trust office services are often employed for tax reasons. Large companies, artists, elite sportspeople and world leaders make use of the services of Dutch trust offices, also enjoying the associated tax benefits it may offer. The Dutch trust sector has a substantial turnover: an estimate by research institute SEO from 2013 puts the annual sums handled by trust offices at around €4,000 billion.[67]

Exports

The Netherlands is the second-largest exporter in the EU. Key export products include machinery and machine components, natural gas, ornamentals (flowers, plants and tree nursery materials) and high-quality synthetics.[68] The combined product exports represent over 20% of the GDP, and this figure rises to over 30% if service exports are included.[69] Service exports comprise mainly logistics, technological and commercial services (royalties and licensing fees).[70] Although only 2% of the Dutch population is employed in agriculture, extensive mechanisation has made the Netherlands into the world's second-largest exporter of food and agricultural products. Nearly 75% of total exports is targeting other EU countries, principally Germany, Belgium, the United Kingdom and France.[71] Most Dutch

63 International Monetary Fund (2017).

64 As at 19 July 2017. Trust offices in the Netherlands must have a licence to operate, and are subject to monitoring by the Dutch Central Bank (DNB) under the Trust and Company Service Providers (Supervision) Act (Wtt). The DNB manages a register of Dutch trust offices.

65 Streiff & Scheltema Beduin (2017).

66 The DNB Statistical News Release from 29 December 2014 puts the number of special financial institutions at 14,400, see: www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/statistisch-nieuws-2014/dnb316987.jsp#.

67 Kerste et al. (2013).

68 www.cbs.nl/nl-nl/nieuws/2017/06/machines-lucratiefste-product-voor-nederlandse-export.

69 European Parliament (2015).

70 Bouman (2016).

71 European Parliament (2015).

imports come from Germany, Belgium, China, the United States and the United Kingdom[72], and constitute principally machines and mineral fuels.[73] 2013 saw an export surplus of €46,751 million.[74]
Large dependencies on exports and the international financial markets meant that from 2009 onwards the Netherlands suffered greatly from the economic crisis, when the economy shrank by 4%.[75] The financial sector suffered in particular, and various banks and an insurer submitted applications for government support.[76] Growth returned to the Dutch economy in 2014.[77]

Unemployment
Unemployment is low in the Netherlands compared to other EU countries. In 2001, only 2.5% of the labour force was unemployed. This figure reached 7.9% in February 2014 due to the crisis, mainly affecting youth, those with little education and people from ethnic migrant backgrounds. Unemployment dropped steadily after that time, reaching 4.7% in June 2017.[78]

3.3 Forms of crimes predicating money laundering

This section looks at the scope and trends in crime directed at the acquisition of assets, including trends in drug-related crime in the Netherlands.

Money laundering can be predicated by various types of crime, the proceeds of which must then be money laundered. These include a broad spectrum of property crimes, along with human trafficking, human smuggling and drug-related crime. This section looks at the spectrum and trends in (recorded) property crimes in the Netherlands in recent years.

Table 3.2 Recorded property crime, human trafficking/smuggling and drug-related crimes from 2014-2016, in figures

	2014	2015*	2016*
*Crimes, total***	*1,025,630*	*978,730*	*928,870*
1 Property crimes	631,450	614,065	576,525
– Theft/misappropriation and burglary	592,590	549,125	498,290
– Deception	19,735	37,410	45,385
– Forgery	9,850	18,400	24,635
– Handling stolen goods	6,940	6,745	5,770
– Extortion and blackmail	1,515	1,635	1,660
– Criminal bankruptcy (bankruptcy due to criminal acts)	170	180	165
– Money laundering	655	570	620
2 Human trafficking, human smuggling	625	615	695
3 Drug-related crimes	16,310	14,810	13,450
– Hard drugs	7,715	7,400	6,770
– Soft drugs	8,195	7,035	6,445
– Drug-related crimes (other)	400	375	230

[72] European Parliament (2015).
[73] https://tradingeconomics.com/netherlands/imports.
[74] €433,106 million in exports as opposed to €386,355 million in imports (European Parliament, 2015).
[75] FATF (2011).
[76] European Parliament (2015).
[77] Eurostat (2016).
[78] CBS Statline (2017).

* The 2015-2016 figures are provisional.

** This includes property crimes, vandalism, disturbance of the order and public authority, violent crimes, sex offences, drug-related crimes, traffic offences, firearm/weapon offences, and other crimes listed in the Dutch Penal Code (WvS) or described in other Acts.

Source: Statistics Netherlands (CBS), Statline

According to CBS data, around 65% of recorded crimes in the Netherlands is financially -related. Table 3.2 shows that recorded property crime has decreased in recent years, and that the crimes most commonly recorded are theft, misappropriation and burglary. Far less but increasing are the registered cases of deception and forgery. Deception refers mainly to conning or frauding; most forgeries are cases of forged documents. A decline in the number of drug-related crimes is visible, however recent years show an evident change in the ratio of hard to soft-drug crimes, with the number of recorded hard-drug crimes exceeding soft-drug crimes from 2015 onwards. Most hard-drug crimes involve possession; most soft-drug crimes involve growing cannabis.[79]
Money laundering is listed in the table as a separate financial crime. CBS data show that around 600 cases of money laundering are recorded by the police each year. However, this figure does not include the cases recorded by the Royal Netherlands Marechaussee or the special investigative authorities, which raises the total amount of money-laundering cases in the Netherlands.[80]

Drug production and drug trafficking

This section has already pointed out that various studies list the Netherlands as a major producer and trade hub for various types of drugs. More details are provided below.

The Netherlands is a major producer of cannabis products,[81] which are exported primarily to the United Kingdom, Germany, Italy and Scandinavian countries.[82] 2015 saw the dismantling of 5,856 hemp farms, which was slightly fewer than in the two preceding years.[83] The Netherlands acts as a key import and distribution hub for the entire EU market. Although these activities sometimes give rise to violence in the form of gang wars, most of the resulting violence between rival criminal organisations is probably the result of growth in domestic production.[84]
The Netherlands is a major producer of synthetic drugs, especially ecstasy[85] and amphetamines.[86] Key destinations for amphetamines are the United Kingdom and Scandinavia, while ecstasy is also exported to Australia.[87] Fifty-nine synthetic drug labs were dismantled in 2015, three times as many as in 2010. A far greater rise has been recorded in waste disposals associated with the production of synthetic drugs, between 2010 and 2015, the number of these recorded waste disposals rose

[79] Van Laar & Van Ooyen-Houben (2016).

[80] The exact number of money-laundering cases registered by the Royal Netherlands Marechaussee and the special investigative authorities could not be ascertained.

[81] E.g. CIA (2017); EMCDDA (2017).

[82] EMCDDA (2017).

[83] Van Laar & Van Ooyen-Houben (2016).

[84] EMCDDA (2016).

[85] Department of State (2017a), CIA (2017), EMCDDA (2017), Van Laar & Van Ooyen-Houben (2016).

[86] Van Laar & Van Ooyen-Houben (2016).

[87] EMCDDA (2017).

from 25 to 160.[88] The CIA also notes that the Netherlands is a major consumer of ecstasy.[89]
The INCSR report states that the Netherlands is a key transit country for cocaine and heroin, which enter the Netherlands principally via the Port of Rotterdam and Amsterdam Airport Schiphol from Peru, Bolivia and Colombia (cocaine) and Afghanistan (heroin).[90] In 2016, a total of 43 tonnes of cocaine was intercepted in the ports and at Schiphol.[91] Varying levels of discipline in registration and the use of differing data systems mean that the recorded data constitute an underestimation of the actual quantities of intercepted drugs.[92]
Drugs trafficking via the 'dark web' doubled between 2013 and 2017, but is still limited in comparison to traditional methods. Cannabis, psychostimulants and ecstasy are traded via the 'dark web' [93], The Netherlands is fifth in the world in this category (after the US, UK, Australia and Germany).

3.4 Factors that make the Netherlands less vulnerable to money laundering

In addition to the above-mentioned factors that render the Netherlands susceptible to money laundering, it also has some characteristics that have the opposite effect. Unlike other countries included in the INCSR report, for example, the Netherlands has comparatively little organised crime, and there is virtually no black market for illegal goods.[94]

Transparency International publishes the annual Corruption Perceptions Index (CPI), which is based on the judgements of experts worldwide on the extent of public-sector corruption in 176 countries. The latest CPI (on the year 2016) rated the Netherlands as the seventh-least corrupt country. The Netherlands therefore has relatively little corruption.[95]

Lastly, it should be mentioned that according to the second FATF follow-up report from 2014, effective measures were taken in the preceding years to combat money laundering in the Netherlands. The main measures included amendments to the Money Laundering and Terrorist Financing Prevention Act (Wwft), updates to the guidelines of the Ministry of Finance and the implementation of a National Threat Assessment for money laundering.[96]

[88] Van Laar & Van Ooyen-Houben (2016).
[89] CIA (2017).
[90] Department of State (2017a), CIA (2017), EMCDDA (2017).
[91] Department of State (2017a).
[92] Van Laar & Van Ooyen-Houben (2016).
[93] Van Laar & Van Ooyen-Houben (2016).
[94] Department of State (2017b).
[95] Transparency International (2017).
[96] FATF (2014).

4 Risks relating to money laundering

This section will firstly discuss various money-laundering threats, while drawing a distinction between *methods* and *channels* (where methods can be applied, either individually or in combination). Next, the results of the first expert meeting will be discussed, in which experts reduced a longlist of threats into the ten risks with the greatest potential impact, and ranked this impact using a multi-criteria analysis (MCA). It concludes with a look at the availability of data on the prevalence of the ten risks identified that are or are not available.

4.1 Introduction

The following research activities were employed to create a longlist of money-laundering threats (see also section 2):

- Analysis of six foreign NRAs,[97] the European SNRA, the NDB and other relevant reports;
- An e-mail questionnaire asking representatives of expert organisations to name the ten money-laundering threats that, in their view, were the most significant;
- Interviews with academics and representatives of expert organisations to gain a better understanding of certain threats (some of which had already been named in the e-mail questionnaire).

Rather than a comprehensive list of all possible money-laundering threats, the longlist was a broad selection of threats resulting from the above-mentioned research activities. The frequency given for each threat in the e-mail questionnaire was used in deciding whether or not to include it on the longlist, and some threats named in the questionnaire were merged together into group threats. To avoid significant threats being left out of the longlist, the experts in the first meeting had the chance to add any money-laundering threats they felt had been overlooked.

Focus on laundering channels and methods

Some foreign NRAs lay the focus on the forms of crime that predicate money laundering, for example the NRA of the US, which include drug trafficking, human trafficking/smuggling and different types of fraud. Rather than these associated predicate offences, the Dutch NRA focuses on the channels and methods used to launder money, for the following reasons:

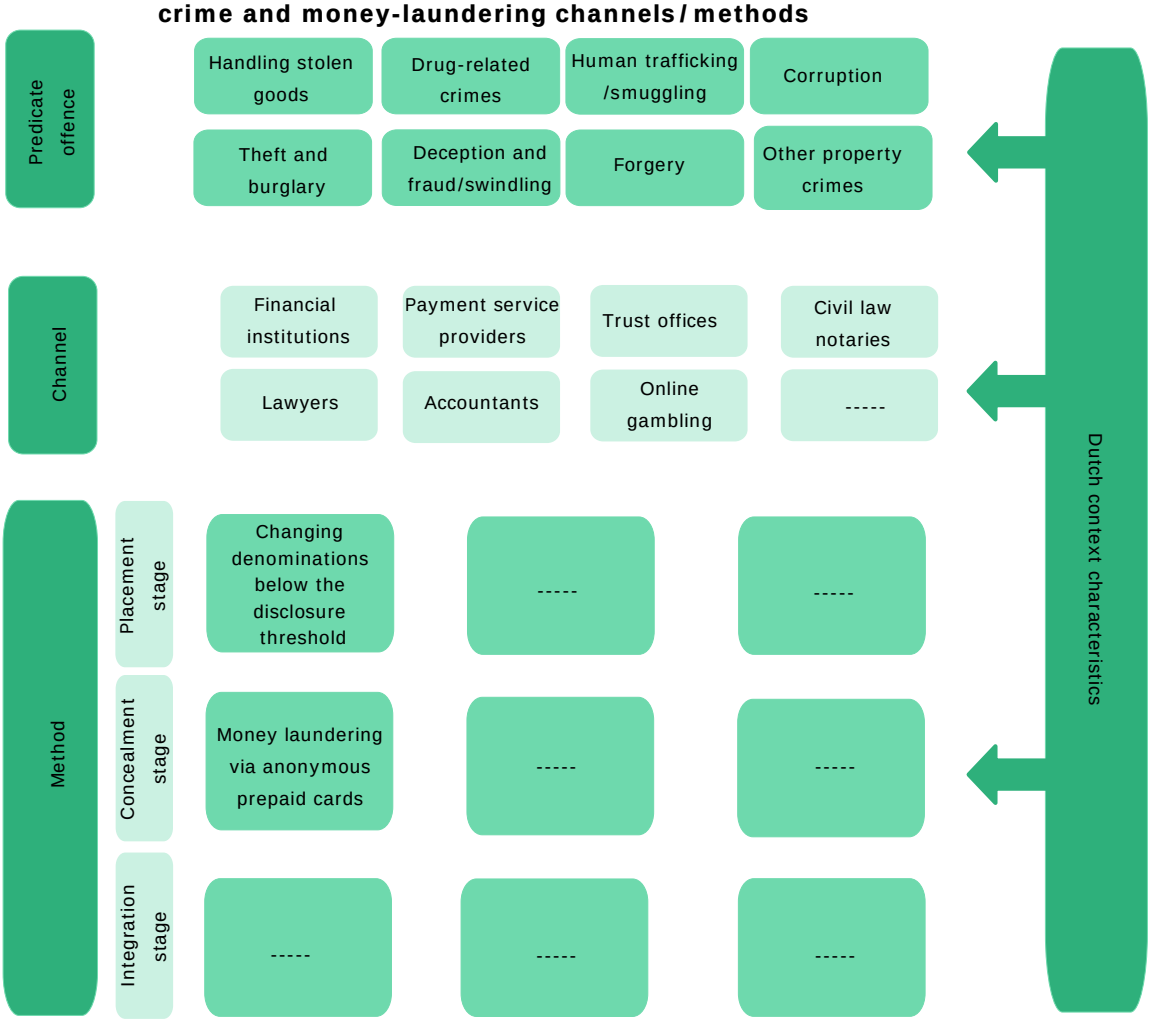
- Focusing on channels and methods rather than the predicate offences reveals the different ways in which money laundering manifests in practice. This provides concrete starting points for generating new policy or enhancing existing policy to combat and prevent money laundering.
- In the questionnaire and interviews, representatives of expert organisations primarily saw money-laundering channels and methods as threats, rather than associated predicate offences.

A plenary discussion during the first expert meeting dealt comprehensively with the question of whether or not to include predicate offences in the NRA. Most experts believed that offences should not be included, as the focus of the NRA should be on

[97] These were the Irish NRA and the five NRAs included in the exploratory study (Van der Veen & Ferwerda, 2016), i.e. those from the US, Canada, the UK, Italy and Sweden.

money laundering and not on the predicate offences. At the start of the first expert meeting, experts were given the opportunity to add threats to the longlist (see also Section 4.3). Although three predicate offences were added to the list, only a few experts selected them as risks with the greatest potential impact.

Figure 4.1 Diagram depicting the relationship between preceding forms of crime and money-laundering channels / methods



The laundering channels can be viewed as the sectors in which the money is laundered. The methods are one level lower than the money-laundering channels: within each channel, multiple methods can be applied. Money-laundering methods can also predicate, follow, or form part of other money-laundering methods. Figure 4.1 depicts the relationship between predicate forms of crime and money-laundering channels and methods.

4.2 Money-laundering channels and methods

The process of money laundering is generally divided into three stages: 'placement' (criminal funds are introduced into the financial system), 'concealment' (the origin of the criminal funds is concealed) and 'integration' (the criminal funds are invested in legal projects, objects or goods). Some money-laundering channels and methods

are principally employed during the initial stage, and others in later stages. This section first describes the various channels used to launder criminal funds, and later describes various methods that predicate, follow, or form part of other methods.[98]

4.2.1 Money-laundering channels

Banks

There are various ways for criminals to take advantage of banking products and services, including: making deposits or transactions below the registration and disclosure thresholds; opening bank accounts whereby agents (or straw men) conceal the identity of the account administrator; exchanging low-denomination banknotes for higher denominations;[99] introducing cash into the electronic payments system permitted under national law; etc.

Payment service providers

Payment service providers are entities other than banks whose business is to provide payment services to end-users. These services may include: supporting and processing debit card transactions; facilitating online payments; issuing and accepting payment cards such as credit cards; and providing international money transfers. Money transfer companies are counted among payment service providers. Under the Financial Supervision Act (Wft),[100] payment service providers must have a licence to operate. In the Netherlands, these licences are issued by the DNB.[101] Under certain conditions[102] some payment service providers may be exempt from needing a permit, if they only offer payment services in the Netherlands and the transactions are of limited size. There are also various international providers operating on the Dutch market that may be located in jurisdictions with less stringent or less current legislation.[103]

Money transfer companies can be used by criminals to launder money. These companies must have either a DNB or EU licence, and a maximum limit applies when sending money via a money transfer company. Criminals not wishing to draw attention can split up large sums into multiple smaller ones, staying below the monetary threshold above which payment service agencies and money transfer offices must report unusual transactions (this is sometimes referred to as 'smurfing').[104] A previous study by the WODC revealed that money transfer companies are often used to launder money obtained from both banking malware and drug trafficking.[105]

Ordinary stores, in particular travel agents, call shops and tobacconists also offer services similar to those of money transfer companies. These are referred to as the 'payment service agencies' of money transfer companies, who must be notified by the DNB (the money transfer company must have a DNB or EU license). The agencies fall under the supervision of the DNB, who is authorised to conduct

---

[98] There may be some overlap between channels and methods (e.g. because some methods make use of one or several channels), however this does not produce any methodological problems.

[99] Although changing denominations is in itself not money laundering, it does facilitate the transport of large sums of criminal funds.

[100] See the bibliography for official titles and sources of legislation.

[101] Dutch Association of United Payment Organisations [*Verenigde Betaalinstellingen Nederland*] (n.d.).

[102] Financial Supervision Act, Section 1a, Exemption Regulations; see the bibliography for official titles and sources of legislation.

[103] Oerlemans et al. (2016).

[104] Oerlemans et al. (2016).

[105] Kruisbergen et al. (2012).

inspections on the premises. Unregistered stores offering money transfer services are illegal. In the past, FIU Netherlands has identified a number of risks pertaining to stores that offer money transfer services: their owners are neither registered with, nor screened by, the DNB. [106] Because these stores are not financial institutions, their employees are often also less familiar with the risks of money laundering than those of regular money transfer companies.

Trust and Company Service Providers (TCSPs)

The Dutch TCSP sector is relatively large, consisting of 224 TCSP offices[107] providing one or more trust services in the course of a business or profession. A TCSP is defined as a legal person, company or natural person that, whether or not jointly with other legal persons, companies or natural persons, provides one or more of the services referred to below in the course of a business or profession.[108] Services offered by TCSP include:

- being a director or partner of a legal person or company on the instructions of a legal person, company or natural person not belonging to the same group as the party who is a director or partner.
- making a postal address or an address available, on the instructions of a legal person, company or natural person not belonging to the same group, to another legal person or company, if at least one of the following additional activities are performed for that legal person or company or for another legal person, company or natural person belonging to the same group as that legal person or company.
- selling or acting as an intermediary in the sale of legal persons.
- being a trustee within the meaning of the Convention on the Law Applicable to Trusts and on their Recognition on the instructions of a legal person, company or natural person not belonging to the same groupmaking use, for the benefit of a customer, of a company belonging to the same group as the party making use of the company. These companies are inter alia used to manage intellectual property, for consultancy services, to trade goods and issue loans.

Due to the nature of the services TCSPs have a high money-laundering risk, since these services are often directed towards the fiscally-driven structures of legal entities which – partly due to their complexity – are vulnerable to misuse. The structure of the legal entities served by TCSPs can be used to conceal assets, or the ultimate beneficial owners. Moreover, the structures of legal entities often cover a range of offshore jurisdictions.

***Politically Exposed Persons* (PEPs)**

Politically Exposed Persons (PEPs) are persons occupying a prominent public office[a] and their families or associates. PEPs represent a risk because they are susceptible to corruption: especially those from highly corrupt countries can use their position to misappropriate government funds or accept bribes. Under the Money Laundering and Terrorist Financing Prevention Act, institutions either entering into a 'relationship' *with,* or conducting transactions *for,* a PEP who is not a Dutch national or a resident of the Netherlands enhanced customer due diligence must be applied. Institutions subject to the provisions of the Act must ascertain whether both their

[106] Kruisbergen et al. (2012).

[107] DNB status as at 19 July 2017. Trust offices in the Netherlands must have a licence to operate, and are subject to monitoring by the Dutch Central Bank (DNB) under the Trust and Company Service Providers (Supervision) Act (Wtt). The DNB manages a register of Dutch trust offices.

[108] Trust Offices (Supervision) Act, Section 1; see the bibliography for official titles and sources of legislation.

client and the ultimate beneficial owner (UBO) qualify as PEPs. The enhanced measures taken as part of the customer due diligence will depend on the institution's risk assessment of the relevant client, transaction or product[b].

[a] People remain PEPs for one year after leaving the prominent position or capacity that originally qualified them as a PEP.

[b] www.afm.nl.

Civil law notaries and lawyers

A money-laundering method that can be applied through civil law notaries and lawyers is the exploitation of so called 'derdengeldenrekeningen', literally third parties' accounts. These accounts are generally used to temporarily secure funds, or to collect funds on behalf of clients. Their purpose is to keep the funds separate from the civil law notary's or lawyer's office assets in order to prevent improper use or bankruptcy. Civil law notaries and lawyers may only use these accounts for transactions in which they are directly involved, i.e. they must have provided services to third parties involving a payment obligation from one party to the other. Criminals can exploit such accounts by concealing criminal proceeds and making them seem legitimate. Lawyers in the Netherlands have no legal obligation to keep a trust account; civil law notaries do, however. In the past, civil law notaries have been convicted for deliberately cooperating with money-laundering activities via these accounts.[109]

Accountants

Criminals can use accountants' services to make money-laundering activities seem legal. The following section describes a variety of such methods, which include purchasing of real estate, setting up a business or foundation or drawing up invoices for transactions for money-laundering purposes (e.g. over/underbilling). Accountants who are insufficiently aware of their clients' criminal activities may unintentionally become accessories to money laundering. In other cases they may indeed be aware of their clients' criminal activities, and intentionally aid in money-laundering practices.[110]

Underground banking

Banking services operating without a licence from the DNB or who do not meet the DNB criteria and have not registered with them are guilty of illegal or 'underground' banking (e.g. Hawala). Criminals may decide to transfer their funds via underground banking, which offers them a number of benefits. International payments, for example, can be made without using official channels, avoiding the risks associated with physical transport (seizure of property) or transfer via the regular banking system (risk of being reported as an unusual transaction). Another advantage for criminals is that underground banking allows for large cash payments and physical transfer of funds, providing many opportunities to launder criminal proceeds.[111]

Online gambling

In a recently published study by the IARM Transcrime project, the Dutch gambling sector was seen as the highest money-laundering risk.[112] Various foreign NRAs also determined that via the gambling sector money laundering may occur. The size of the risk is not always estimated. Online gambling is still illegal in the Netherlands, with the exception of the e-commerce activities by a few parties. This situation is

[109] www.advocatie.nl/oud-notaris-kloeck-krijgt-vier-jaar-cel-voor-rol-vastgoedfraudezaak-klimop.

[110] European Commission (2017).

[111] Kruisbergen et al. (2012).

[112] Savona & Riccardi (2017).

set to change with the *Kansspelen op Afstand*, or KOA, part of the new Betting and Gaming Act, which was adopted by the Lower House in July 2016 and has been presented to the Senate. KOA will regulate the provision of online gambling in the Netherlands, setting a range of criteria to which the provider and the organisation of the games must comply. The legislation aims to reduce both the vulnerability of the players and the money-laundering risks.[113] It should be noted that the KOA does not affect illegal online gambling providers operating in unregulated foreign territories. A study by Decision Support on money-laundering risks in the gambling sector designated unregulated online gambling as a money-laundering risk.[114]

4.2.2 Money-laundering methods

Payment methods

Money can be laundered in many ways using *cash*. Examples include: changing denominations below the monetary threshold[115] of banks or payment institutions; depositing large sums with banks or payment service providers below the monetary threshold; and converting cash into valuable goods, such as precious metals or artworks. It is of course much easier for criminals to launder money via institutions that are not obliged entities than via entities, where any payments or transactions must remain below the monetary threshold. Another example of money laundering using cash is its physical transport to or from the Netherlands, e.g. via money couriers or by using regular postal services.[116] A 2015 Europol study revealed that the laundering of criminal proceeds using cash is relatively common. However, investigative authorities say mapping out the actual scope of the problem is difficult, since the nature of cash money (as well as the volume and denominations in circulation) means there are little concrete data available.[117]

Another money-laundering method involves the use of *virtual currencies*. In 2016 there were about 500-600 virtual currencies in use, [118] including bitcoin, monero and ethereum. Virtual currencies do not fall under the authority of any single country, central bank or other financial supervisory body. Criminal proceeds may be laundered fairly anonymously. A previous study by the WODC pointed out that criminals can increase the anonymity of bitcoins by using a 'mixing service', after which they can be transferred to a bitcoin address belonging to one or more intermediaries, allowing the criminal to further convert and/or spend them.[119] At least three criminal cases emerged in 2017 in which the Public Prosecution Service prosecuted the trade and exchange of bitcoins as money laundering. The Fiscal Intelligence and Investigation Service (FIOD) has detected criminal traders and 'bitcoin-cashers' on the dark web (who exchange bitcoins for cash in return for a fee).[120]

In addition to cash and virtual currencies, anonymous prepaid cards also form a money-laundering method. These cards exist in various forms, such as prepaid telephone cards, gift cards and vouchers for products or services. Users can remain anonymous, as no identification is requested from either the purchaser or the user. Criminals can anonymously charge the cards with illegal or criminal proceeds, and

---

[113] Van der Knoop (2017).

[114] Van der Knoop (2017).

[115] This refers to the existing indicators that apply to reporting unusual transactions.

[116] Kruisbergen et al. (2012).

[117] Europol (2015).

[118] European Parliament (2016).

[119] Oerlemans et al. (2016).

[120] https://fd.nl/economie-politiek/1181589/om-voert-strijd-op-tegen-witwassen-via-bitcoin.

spend them later in a store or online. The cards can also be easily transported in and out of the EU, as there is no obligation to declare them at customs. There is an obligation to declare cash, however: an EU regulation[121] stipulates that people entering or leaving the EU with €10,000 or more in cash must declare it at customs. There is currently a proposal to amend this regulation, which would include prepaid cards under the definition of 'cash' (liquid assets).[122]

Money-laundering constructions

Various financial and other constructions are available to criminals for money-laundering purposes, a selection of which are described in this section.

- *Loan-backs.* One example of a financial construction used to launder money is the loan-back. Using this method, criminals loan money to themselves via a certain route (e.g. via a corporate entity) in such a way that to the outside world, it is not apparent that the issuer and recipient of the loan are the same person.[123]
- *Stacked corporate entities*. Criminals can use complex corporate structures to launder money. One way they conceal money laundering is by setting up a chain of different public and/or private limited companies that make payments to one other.
- *Offshore companies*. An offshore company is based in a country that does not require the registration of beneficial owners or transactions, and where criminals can therefore store large sums of money unnoticed. The offshore company has its own bank account, and can therefore retransfer funds to the criminal e.g. as a mortgage loan or to a private limited company under its control. According to Koningsveld, at the end of 2013 around €5,565 billion had been deposited in offshore banking institutions, roughly one-quarter of all banking capital worldwide. Van Koningsveld believes it is reasonable to assume that this offshore capital goes undeclared either wholly or in part to the tax authorities in the owners' country of residence. He estimated that the Netherlands thus loses €10 billion in tax revenue annually.[124]
- *ABC transactions.* There are various known money-laundering transactions in the real estate sector, one of which is known as the so-called ABC transaction. FIU Netherlands defines this construction as the sale of a premises at least twice within a period of no more than six months. This is a common occurrence in practice, and the FIU Netherlands says there is usually no money laundering at play, however such ABC transactions are sensitive to money laundering.[125]
- *Investment constructions*. Investment constructions also offer money-laundering opportunities for criminals, who can make the investment process very convoluted to obscure their actions. For example: criminal funds can first be deposited into a bank account in a foreign country where supervision and monitoring are less stringent; after that, it can be transferred to an investment account in the

---

[121] See the bibliography for official titles and sources of legislation.

[122] See the bibliography for official titles and sources of legislation. The proposed amendment to the Fourth EU anti-Money laundering Directive also includes an expansion of the customer due diligence obligations for certain prepaid instruments, including lowering the mandatory customer due diligence monetary threshold when charging prepaid methods from €250 to €150, and eliminating a qualified exception to the customer due diligence obligation when using prepaid methods online.

[123] Kruisbergen et al. (2012).

[124] https://fd.nl/economie-politiek/1121518/promovendus-politie-en-fiscus-moeten-meer-aandacht-schenken-aan-misbruik-offshores; Blauw, 30 January 2016, no. 1. *Crimineel vermogen in belastingparadijs is onzichtbaar* [Criminal proceeds in tax havens are invisible].

[125] FIU Netherlands. Information sheet: *Hoe meld ik een ABC-transactie aan FIU-Nederland* [How to report an ABC transaction to FIU Netherlands].

Netherlands under a code name or number instead of the real account-owner's name. A friendly stockbroker can then start using the numbered bank account; any profits made can be transferred to a third account, where the owner then receives the laundered funds. Any bad investments can be deducted from the numbered account, and provided the losses do not significantly outweigh the profits, the primary goal of laundering illegal funds is achieved.[126]

Trade-Based Money Laundering (TBML)

Trade-Based Money Laundering (TBML) is a practice that makes use of national and international trade (and sometimes financial institutions) to launder criminal proceeds. The criminals set up businesses and use commercial transactions to launder the funds. TBML has several forms:

- *Legitimisation of value transfer or growth/loss in value via commercial transactions.* National and international trade offers opportunities for commercial transactions by criminals to transfer value or to legitimise growth or loss in value. In such cases it is unclear whether transactions are associated with a goods flow, what the origin of the goods flow is, and/or whether a goods flow even exists.
- *Over/underbilling.* In practice, two businesses can collaborate closely to launder money. One such method involves overbilling, when one business overbills another for the purchase of a product or service. By making the total value of the transaction higher than the actual price of the product or service, the billing company that receives payment attempts to attribute a legal origin to the additional funds. The businesses can also launder money by sending multiple invoices to each other for products or services that are only supplied once.
- *Turnover/price manipulation.* One method associated with that described above is turnover/price manipulation, when the billing company lowers the price of a product or service in order to give the receiving company a legal financial benefit.[127]

Concealing identity through straw men

Straw men (or 'money mules') can be used by criminals in a range of money-laundering methods, allowing them to conceal their identity. Straw men are used in the real-estate sector, for example, to shift legal ownership from the launderer (who is the beneficial owner) to the straw man. Expenditure can also involve a straw man, e.g. when criminals make purchases via another person's (i.e. the straw man's) bank account.

4.3 Identifying the ten risks with the greatest potential impact

The previous section offered a brief description of the longlisted money-laundering channels and methods. This section outlines the results of the first expert meeting, in which the experts were asked to select the ten threats from the longlist that they believed had the greatest potential impact. Sixteen experts were present at the first meeting.

[126] www.trouw.nl/home/beurs-biedt-alle-gelegenheid-tot-misbruik-en-witwassen~af5b7619/.

[127] http://juridischactueel.nl/het-gevaar-van-trade-based-money-laundering/.

4.3.1 Additions and modifications to the longlist

First of all, the experts were given the chance to supplement the longlist that was drawn up by the WODC with any threats they thought had been overlooked, which resulted in the following additions:

- *VAT abuse (e.g. VAT carousel fraud).* VAT carousel fraud involves charging customers VAT, but not paying it to the tax authority.
- *Identity fraud.* Criminal use of forged or stolen identity information.
- *Bankruptcy fraud.* This type of fraud is committed by or while allowing a business to go bankrupt.
- *Abuse of foundations.* The experts pointed out that foundations can be used to launder criminal funds while concealing the real owner's identity, and have observed an increase in the number of foundations apparently being used for this purpose.

Several participants disagreed with the addition of the first three threats to the longlist, as they believed the relevant crime was ‘fraud’, not specifically ‘money laundering’. A plenary discussion resulted in the decision to add them regardless, as the experts would still have the opportunity *not* to include these threats in their personal lists of the ten threats with the greatest potential impact. The additional threats were ultimately selected by only a few participants (3 for identity fraud, 2 for VAT abuse, and 1 for bankruptcy fraud).

The discussion also resulted in the modification of two threats that were already on the longlist:

- The initial version of the longlist included ‘Expenditure at non-obliged entities’. The participants stated that it was not only expenditure, but also the transfer of assets to these entities that represent a threat. The wording was adjusted as follows: ‘Expenditure at and transfer of assets to non-obliged entities’.
- In consultation with the experts, it was decided to reformulate ‘Abusing the services of money-transfer companies’ more generally to ‘Abusing the services of payment service providers’, as there are several types of entities that provide payment services, not just money-transfer companies.

See below for the final longlist of threats from which the experts could select the ten threats which, according to them, have the greatest potential impact.

Table 4.1 Longlist of money-laundering threats

Money-laundering channels	
Financial institutions (especially banks)	Civil law notaries (abuse of third parties' accounts)
Trust offices	Lawyers (abuse of third parties' accounts)
Payment service providers (organisations offering payment services either with or without a licence)	Accountants
	Online gambling
Money-laundering methods	
Trade-Based Money Laundering (TBML): National and international commercial transactions offering opportunities for criminals to transfer value or to legitimise growth or loss in value and obscuring whether transactions are associated with a goods flow, what the origin of the goods flow is, and/or whether a goods flow even exists	Physical relocation of cash funds to/from the Netherlands, through underground/unlicensed banking or otherwise
Over/underbilling within national/international commerce (falls under TBML)	Introducing cash funds into the electronic payments system
Turnover/price manipulation (falls under TBML)	Converting cash funds into valuable goods
Using national/international investment structures for value transfer	Large cash deposits
Constructions for concealing actual value	Exchanging small cash denominations for larger ones (and vice versa)
Offshore companies	Virtual currencies
ABC transactions	Prepaid cards, debit cards, telephone cards, etc.
Straw men	Fiscally-driven/complex corporate structures
VAT abuse	Purchase/renovation of real estate using dirty money or untraceable funds
Identity fraud	Expenditure below the monetary threshold by obliged entities
Bankruptcy fraud	Expenditure at and transfer of assets to non-obliged entities
Abuse of foundations	Non-transparent cash flows from abroad (PEPs)
Transferring cash funds through underground/unlicensed banking (e.g. Hawala)	

4.3.2 Identifying the ten risks

The experts were asked to select the ten threats from the modified longlist that they believed had the greatest potential impact. A plenary session was then held to discuss the threats that made it to the top ten and which would elevate the status of these threats to 'risk', and the threats that did not make it to the top ten. The participants had the opportunity to provide arguments for why certain threats that did not reach the top ten should be included after all. One of the experts argued that 'money laundering via virtual currencies' (which did not make it to the initial list of the greatest risks) was one such threat. The expert stated that, although he believed there were no concrete figures indicating the prevalence of the use of virtual currencies to launder criminal proceeds, he nonetheless saw it as a significant potential risk.

After the plenary session, the experts had the chance to revise their original selection. The first expert meeting produced the following list of ten money-laundering-related risks (see Table 4.2). Three threats were selected by ten of the sixteen experts. After discussion, it was decided not to include 'straw men' in the list of risks, as the experts believed it could be an element in a variety of other risks on the list containing the greatest risks. Seven of the ten risks were selected by at least three-quarter of the experts, and the other three by around two-thirds of the participants. Seven of the risks are money-laundering methods, and the other three relate to money-laundering channels.

Table 4.2 The experts' top ten money-laundering-related risks*

	% of experts (n=16)	Money-laundering channel	Money-laundering method
Trade-Based Money Laundering: national and international commercial transactions offering opportunities for criminals to transfer value or to legitimise growth or loss in value and obscuring whether transactions are associated with a goods flow, what the origin of the goods flow is, and/or whether a goods flow even exists	94%		O
Money laundering via offshore firms	94%		O
Money laundering via trust offices	88%	O	
Money laundering via payment service providers	81%	O	
Money laundering via fiscally driven/complex corporate structures	81%		O
Money laundering via virtual currencies	81%		O
Money laundering via financial institutions (especially banks)	75%	O	
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	69%		O
Money laundering constructions to conceal actual value	63%		O
Money laundering via national and international investment structures for value transfer	63%		O

* The risks in this table are formulated more concisely than in Table 4.1, however they are the same threats/risks.

During the meeting, the experts were given the opportunity to further explain and discuss their ten risks with one another, resulting in the following observations:[128]

- *Trade-Based Money Laundering: national and international commercial transactions offering opportunities for criminals to transfer value or to legitimise growth or loss in value and obscuring whether transactions are associated with a goods flow, what the origin of the goods flow is, and/or whether a goods flow even exists.* During the meeting it was discussed whether this risk should be merged with 'national and international investment structures for value transfer'. Although one of the experts felt that both cases involve Trade-Based Money Laundering, other experts disagreed, saying that 'national and international investment structures for value transfer' does not qualify as TBML because investments are

[128] During the meeting, the experts did not provide any further details regarding 'money laundering via trust offices' or 'money laundering constructions to conceal actual value'. These risks are explained in more detail in Section 4.2.

not commercial transactions involving goods trading. In consultation with the experts it was ultimately decided not to merge the two risks.[129]

- *Money laundering via offshore firms.* During the expert meeting, reference was made to the aforementioned study by Van Koningsveld. As mentioned in the section above, Van Koningsveld estimates that the Netherlands loses around €10 billion in tax revenue annually through offshore firms.
- *Money laundering via payment service providers.* All transactions by licensed money-transfer companies must be reported to the DNB, which is evidence of the high risk of money laundering in the sector, according to the experts. They did note, however, that the average money-transfer amount is not especially high (approximately €300), limiting the risk impact. Another point raised during the expert meeting was the fact that both licensed and unlicensed payment service providers were used to launder criminal proceeds.
- *Money laundering via fiscally-driven/complex corporate structures*. Experts in the meeting explained that this risk can involve 'stacked' public or private limited companies for the purposes of concealing money laundering. This method has already been described in the previous section.
- *Money laundering via virtual currencies.* During the meeting, the experts explained that criminal assets converted to virtual currencies are principally used to further other criminal activities, such as the online purchase of drugs and weapons.
- *Money laundering via financial institutions (especially banks).* During the expert meeting, it was noted that the services of financial institutions, especially banks, are exploited relatively often due to the large sums that are moved around the financial sector. Insurance and pension fund services are also exploited, however the experts deemed this risk to be smaller than for banking services.
- *Money laundering via the relocation of cash funds to/from the Netherlands (via underground banking or otherwise).* It was stated during the meeting that large sums of cash enter and exit the Netherlands and the EU each year. According to one expert, there are currently 5,000 Dutch cases and 50,000 European cases per year in which travellers transport more than €10,000 in cash. However, it is unclear whether these are money-laundering cases or not. It was also noted in the expert meeting that straw men are being used increasingly and more often for deposits and transactions of cash funds than for the other risks.
- *Money laundering via national and international investment structures for value transfer.* During the expert meeting it was cited that this method is used as a simple means for storing money before reintroducing it into regular circulation. It was also noted that this risk pertains mainly to the unregulated investment constructions that do not fall under the supervision on the basis of the Financial Supervision Act and/or the Money Laundering and Terrorist Financing Prevention Act.

4.3.3 Estimating the potential impact of risks

After producing the list, the experts were asked to estimate the extent to which each of the risks could have a potential impact on the following seven criteria that form the basis of a Multi-Criteria Analysis (MCA):

- the stability of the financial system;
- the regular economy;
- society (civil and legal order);
- the degree to which regular society is interwoven with the criminal underworld;
- the manifestation or facilitation of crime or terrorist activities;

[129] The remainder of this report refers only to Trade-Based Money Laundering, i.e. without the extended explanation.

- the (perceived) feeling of safety;
- the image/reputation of the Netherlands.

First of all the experts were asked to weight each criterion from 1-10, to express the importance of each criterion relative to the others.[130] This exercise revealed that the experts allocated the most weight to 'the degree to which regular society is interwoven with the criminal underworld' (8.3 on average), and the least weight to 'the (perceived) feeling of safety'. The standard deviations were also calculated, revealing the spread of the experts' judgements. The table shows a relatively large spread, one explanation for which could be the composition of the expert group. The combined and sometimes complementary fields of expertise brought together in the expert group were intended to represent the entire money-laundering spectrum. The various experts' perspectives on money laundering are reflected in the weighting spread, as shown in Table 4.3.

Table 4.3 Expert weighting of the criteria

Criteria	Average score	Standard deviation
The degree to which regular society is interwoven with the criminal underworld	8.3	1.2
The manifestation or facilitation of crime or terrorist activities	7.8	1.8
The stability of the financial system	7.6	1.8
Society (civil and legal order)	6.9	2.4
The regular economy	6.7	1.5
The image/reputation of the Netherlands	6.3	2.9
The (perceived) feeling of safety	4.4	2.4

The experts were then given two opportunities to rate the potential impact of each of the ten risks on a scale from 0-100 i.e. before and after a joint discussion on the risks. After the discussion, the experts were once again asked to estimate the potential impact of the ten risks, in accordance with the Delphi method. The difference between the first and second rounds proved to be very small – only two of the risks' scores differed from one round to the other.

The potential impact of the money-laundering risks after the MCA ranged from 73 to 55 (out of 100). Although differences between the risks were identified, the maximum and the minimum risk levels were relatively close to each other. Some of the risk levels were extremely close, and the estimates were not fully substantiated by the experts.[131] The risks are therefore presented in bracketed ranges in Table 4.4, which shows a potential impact level (after the second round) of 55-60 for six of the risks; 61-70 for three of the risks, and slightly over 70 for the remaining risk. The detailed MCA calculations are given in Appendix 6.

[130] Box 2.2 explains the MCA process, as well as how the criteria are weighted.

[131] The criteria-based approach taken in the MCA and the frequency-based approach shown in Table 4.2 do result in some difference to the ranking of the laundering risks. These differences are not great, however; the positions of seven of the ten risks differ by no more than two places.

Table 4.4 Potential impact of the top ten money-laundering risks (after the MCA)

Risk	Potential risk level (scale from 0-100)
Money laundering via financial institutions (especially banks)	71-75
Money laundering via payment service providers Money laundering via trust offices Money laundering via offshore firms	61-70
Money laundering constructions to conceal actual value Trade-Based Money Laundering Money laundering via fiscally driven/complex corporate structures Money laundering via virtual currencies Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise) Money laundering via national and international investment structures for value transfer	55-60

4.4 Availability of data on the identified risks

After the first expert meeting, a brief e-mail questionnaire was conducted among the participants, asking them to indicate:

- what *existing* data provide information on the scope of the actual prevalence of the ten risks;
- which of the above data are available to third parties; and
- on the basis of what - still missing - data some information may be provided on the current prevalence of the ten identified risks.

Only a small number of experts (six) completed the questionnaire. Two replied saying they found the questions difficult to answer and the remaining eight did not respond to the questionnaire invitation.
Those that did respond referred to unspecified data from the AFM, DNB, the Tax and Customs Administration, the police and Customs, as well as to transaction data of financial institutions, numbers of confirmed violations under the Money Laundering and Terrorist Financing Prevention Act, criminal investigations, and conviction figures with relation to the various risks. One of the experts suggested that data from the land register (*Kadaster*) may offer some insight into the prevalence or scope of the real-estate-related risks.
The questionnaire responses provided no clarity on the availability to third parties of the data cited. A few experts were under the impression that the (rarely specific) data they cited was not available to third parties due to privacy legislation or supervisory confidentiality agreements. One of the experts believes that land register data are indeed available to third parties.
Lastly, the experts gave an indication of the basis of what - still missing - data some information may be provided on the prevalence of the ten identified risks. Answers here were also scarce: one of the experts offered the general suggestion that collating all data from financial institutions might offer a better overview of transactions that could provide information on the relevant risks. Another expert suggested that the future UBO register and the central shareholder's register might be of help in identifying the UBOs of offshore companies.

It is clear from the above that the e-mail questionnaire conducted among the experts produced only limited information on the available and desired data regarding the relevant risks.

5 Resilience of policy instruments

First of all, this section discusses the organisation of the activities aimed at preventing and combating money laundering in the Netherlands, followed by an outline of the available policy instruments. Lastly, the results of the second expert meeting are presented, in which the experts assessed the resilience of the policy instruments that are in place to combat the ten risks with the greatest potential impact.

5.1 Organisation of anti-money laundering activities

Many parties are involved in preventing and combating money laundering in the Netherlands. The Ministry of Finance and the Ministry of Security and Justice are responsible for the central coordination and management of anti-money laundering activities.

Six supervisory bodies are active under the Money Laundering and Terrorist Financing Prevention Act (Wwft):

- the Dutch Central Bank (DNB) monitors banks, financial institutions, lessors of safe-deposit boxes, currency exchangers, life insurance companies, trust offices, payment service providers and agencies, electronic money institutions (EMIs) and leasing companies.
- The Financial Supervision Office (*Bureau Financieel Toezicht*, BFT) monitors civil law notaries, accountants, commercial advisers, tax consultants, independent legal specialists and administrative offices.
- The Wwft Supervision Office (*Bureau Toezicht Wwft*) monitors real-estate agents, registered office providers, appraisers and high value dealers.
- The Netherlands Authority for the Financial Markets (AFM) monitors investment companies/institutions and financial service providers who act as intermediaries for life insurance contracts.
- The district deans of the various bar associations monitor lawyers who provide services falling under the Wwft, which include consultancy for the purchase and sale of businesses, the setup and management of corporate and legal entities, and financial management.
- The Dutch Gaming Authority (Ksa) supervises casinos.

The financial institutions and designated non-financial businesses and professionals listed above have a reporting obligation under the Wwft: they must report unusual transactions to FIU Netherlands, and are also obliged to conduct customer due diligence (see below for more details). FIU Netherlands detects suspicious transactions from the set of unusual transactions, forwarding them to the various (special) investigative, intelligence and security authorities. These suspicious transactions are among the collected indications of money laundering, and can be used for investigative and research purposes. The Financial and Economic Crime Sections of the regional police units, the Fiscal Intelligence and Investigation Service (FIOD) and the National Investigation Service (DLR) all play a key role in criminal investigation activities. Suspected money launderers can be prosecuted by the Public Prosecution Service, and potentially brought to trial. The Public Prosecution Service is also responsible for confiscating assets obtained via criminal means.

Various collaborative frameworks have been established to prevent and combat money laundering. The Criminal and Unexplained Assets Infobox (iCOV) is a partnership between the National Police, the Tax and Customs Administration, Customs Netherlands, the Central Judicial Collection Agency (CJIB), FIU Netherlands, special investigative authorities and the Public Prosecution Service, that provides the member organisations with data intelligence products. iCOV also develops risk indicators and patterns with the aim of exposing money laundering and fraud constructions. The Financial Expertise Centre (FEC) is a partnership between the AFM, the Tax and Customs Administration, the DNB, FIU Netherlands, the FIOD, the Public Prosecution Service and the National Police, whose aim is to strengthen the integrity of the financial sector through preventive action against integrity threats. The FEC also works to boost the effectiveness of the FEC partners through education, information provision and mutual exchange of insights, knowledge and skills.

In addition to the above frameworks, some of the organisations also collaborate in other ways:

- The Anti Money Laundering Centre (AMLC) is a platform facilitating the exchange of knowledge and experience and operational collaboration among parties involved in combating money laundering. The members include the FIOD, Police, Public Prosecution Service, FIU Netherlands and the special investigative authorities.
- Ten Regional Information and Expertise Centres (RIECs) have been established in the Netherlands with a view to combating serious and organised crime. These organisations bring together the information, expertise and strengths of the various government bodies such as municipal and provincial authorities, the Public Prosecution Service, National Police, Tax and Customs Administration (including the Benefits division), Customs Netherlands, the FIOD, the Social Affairs and Employment Inspectorate, Royal Netherlands Marechaussee and the Immigration and Naturalisation Service (IND). The National Information and Expertise Centre (LIEC) provides support and facilitation services.
- Through Integrated Confiscation Teams, police can seek collaboration with parties including the Public Prosecution Service, FIOD, Tax and Customs Administration, and municipal authorities. By bringing together shared knowledge, the Integrated Confiscation Teams aim to improve effectiveness in the confiscation of criminal proceeds via criminal prosecution or fiscal and public administration channels.
- The Unusual Transaction Committee meets twice a year. Sector/umbrella organisations of obliged entities, Wwft supervisory authorities, the Public Prosecution Service and FIU Netherlands meet with representatives from the ministries of Finance and Security and Justice to discuss matters such as the structure and enforcement of the obligation to report unusual transactions, and to decide on the indicators used to determine whether transactions qualify as unusual.

Due to the international character of many money-laundering risks, FIU Netherlands, the supervisory bodies and other law enforcement agencies such as . the Tax and Customs Administration collaborate with international organisations such as Europol and the European body for the enhancement of judicial co-operation (Eurojust) to achieve effective prevention and combat of money-laundering risks. FIU Netherlands is a member of the Egmont Group, an international partnership of FIUs whose main aim is to enhance international data exchange.

5.2 The available policy instruments

The available policy instruments targeting the prevention and/or combat of money laundering include the relevant instruments stemming from municipal, national and international legislation, sector-oriented regulations, and regulations within organisations.[132]

FATF and the EU Anti-Money Laundering Directive
Dutch anti-money laundering policy is based on the recommendations by the FATF, whose members including the Netherlands have committed themselves to implement the forty recommendations for taking measures to prevent and combat money laundering and strengthening national legal and regulatory frameworks and international cooperation. The FATF also monitors the technical compliance and effectiveness of its members in implementing the standards. The EU has transposed the majority of the FATF's recommendations into the fourth Anti-Money Laundering Directive, thus establishing regulations for all EU member states with a view to preventing the financial system from being used for money laundering and terrorist financing. In the Netherlands, these regulations have been implemented into the Money Laundering and Terrorist Financing Prevention Act (Wwft). First and foremost, the implementation of the Fourth EU Anti-Money Laundering Directive will result in amendments to the Wwft.[133] It replaces the Third Anti-Money Laundering directive, and further supplements the existing instruments in this area. Moreover, the Directive prolongs the two core obligations under the Wwft, i.e. obligation to conduct customer due diligence and to report unusual transactions to FIU Netherlands. A Fifth EU Anti-Money Laundering Directive is now under preparation. On 5 July 2016, the European Commission presented a directive proposal with amendments to the Fourth EU Anti-Money Laundering Directive.[134]

Money Laundering and Terrorist Financing Prevention Act (Wwft) [135]
This Act aims to prevent the use of the financial system for money laundering and terrorism-financing purposes, by imposing obligations on financial institutions and designated non-financial businesses and professionals (see also previous section). One such obligation is to conduct customer due diligence, which involves identifying the client and verifying its identity, as well as identifying the client's UBO and taking reasonable measures to verify its identity as well. These entities are under the obligation to report unusual transactions to FIU Netherlands. The data stream thus produced may also aid police and investigative authorities in the identification of money-laundering activities, thereby providing an instrument for combating such activities. There are objective indicators and one subjective indicator for determining whether transactions qualify as ‘unusual’ and require to be reported. One example of an objective indicator is ‘cash exchanges of €15,000 or more’; the subjective indicator is ‘transactions that give an entity reason to assume that it may be linked to money laundering’.

---

[132] The legislation covered in this section was raised and discussed by the experts during the second expert meeting, and serves as an overview of the legislation considered important by the experts in preventing and combating money laundering. It should not be considered exhaustive, however, as it does not include the Code of Criminal Procedure which regulates the criminal proceedings of criminal offences and the Legal Entities Supervision Act (*Wet controle op rechtspersonen)* aimed at preventing and combating misuse by legal entities, among others.

[133] Draft proposal on the implementation of the Fourth EU Anti-Money Laundering Directive; see: www.internetconsultatie.nl/implementatiewetvierdeantiwitwasrichtlijn/berichten.

[134] See the bibliography for official titles and sources of legislation.

[135] See the bibliography for official titles and sources of legislation.

The Wwft takes a risk-based approach: in many cases, entities must themselves assess the risk that a client is laundering money, and adapt the stringency of their own measures accordingly. These measures may vary from a simplified customer due diligence to the refusal to enter into business relations or termination thereof.

Financial Supervision Act (Wft)[136]

The Financial Supervision Act (Wft) entered into force on 1 January 2007, and regulates monitoring of the financial sector in the Netherlands. Financial supervision preserves the stability of the financial system, ensures the efficient operation of the financial markets, and protects consumers against the bankruptcy or unacceptable conduct of financial institutions. The DNB and AMF implement supervision under the Wft:

- It is the responsibility of the DNB to provide 'prudential supervision' of financial companies, and take decisions regarding these companies' access to the financial markets. Prudential supervision focuses on the soundness of financial companies, and aims to enhance the stability of the financial sector.
- It is the responsibility of the AFM to provide 'market conduct supervision' in financial markets, and take decisions regarding financial companies' access to these markets. Market conduct supervision focuses on orderly and transparent financial market processes, clear relations between market parties, and the careful treatment of clients.

Dutch Penal Code (WvS)[137]

On 6 December 2001, money laundering became an independent criminal offence that no longer required conviction of a predicate offence such as drug or human trafficking. The Dutch Penal Code (WvS) specifies the following forms of money laundering:

- Money laundering is defined as intentional if 'at the time of the offence, the offender knows that the object he/she hides or conceals was obtained through criminal activity' (Article 420(b));
- Self-laundering concerns the acquisition or possession of objects derived from crimes perpetrated by the offender (Article 420(b)(1)).
- Habitual money laundering involves repeated intentional laundering, or laundering while practising a profession or running a business (Article 420(c));
- Culpable money laundering requires proof that the offender could reasonably be expected to have known that the object originated from criminal activity, and that the offence was intentional (Article 420(d));
- Lastly, culpable money laundering consisting only of the acquisition or possession of objects derived from crimes perpetrated by the offender (Article 420(d)(1)).

Trust and Company Service Providers (Supervision)Act (Wtt)[138]

The Trust and Company Service Providers (Supervision) Act (Wtt) entered into force on 1 March 2004, and aims primarily to strengthen the integrity of TCSPs. Under the Wtt, TCSPs are to act as 'gatekeepers', by identifying and managing integrity risks. In this context, the Wtt sets criteria for the suitability and reliability of the policymakers, the representation frameworks, and the sound operational practices at TCSPs. These also include the customer due diligence obligations under the Regulations governing Sound Operational Practices under the Trust and Company Service Provider (Supervision) Act (*Regeling integere bedrijfsvoering Wet toezicht*

[136] See the bibliography for official titles and sources of legislation.

[137] See the bibliography for official titles and sources of legislation.

[138] See the bibliography for official titles and sources of legislation.

trustkantoren) 2014. Under the Wtt, TCSPs are obliged to have knowledge of the origin and destination of the funds/financial flows they facilitate. TCSPs that meet the statutory criteria governing the suitability of policymakers and the business operations and organisation of TCSPs receive a licence from the DNB. It is illegal to run a TCSP in the Netherlands without a licence.

European legislation

- *EU Anti-Money Laundering Directive.* See above for an outline of this Directive.
- *EU Regulation on Controls of Cash*. In 2007, it became compulsory for all natural persons entering or leaving the territory of the EU member states carrying €10,000 or more in liquid assets (either cash or marketable instruments to the bearer) to make a declaration to the competent customs or other authorities of the member state where they enter or leave the EU.[139] There is currently a proposal to amend this regulation, which would include prepaid cards under the definition of liquid assets.[140]
- *Wire Transfer Regulation 2*. In June 2017, the new Wire Transfer Regulation (WTR2) came into effect, which is based on a recommendation by the FATF. The WTR2 obliges all payment service providers and intermediary payment service providers to record information not only about the sender, but also the recipient. More stringent obligations were also introduced for payment products that can be used anonymously, or are not in anybody's name.[141]

Other legislation

- *Tax legislation.* The Dutch Tax and Customs Administration uses tax legislation to monitor unexplained assets and foundations with so called ANBI status.[142] This legislation can therefore contribute to preventing and combating money laundering. The experts also mentioned that tax legislation is important for combating money laundering via trust offices, much of whose work is fiscally driven.
- *The Public Administration Probity Screening Act*.[143] The Public Administration Probity Screening Act (*Wet Bibob*) is an (preventative) administrative instrument that applies to (certain) licences, subsidies, expenditure and real-estate transactions. Authorities may decline or withdraw a licence wherever there is a serious risk that the licence may also be used to commit criminal offences or employ criminal funds, thus preventing the government from facilitating criminal activities while also protecting the competitive position of legitimate businesses.
- *Commercial Register Act 2007*.[144] The Commercial Register Act (*Handelsregisterwet*) that entered into force on 1 January 2008 contains stipulations regarding mandatory registration in the commercial register at the Chambers of Commerce. It applies not only to companies, but also to all Dutch public and private legal entities and their branches. Under the Fourth EU Anti-Money Laundering Directive, EU member states must set up a central register of

[139] See the bibliography for official titles and sources of legislation.

[140] See the bibliography for official titles and sources of legislation.

[141] See the bibliography for official titles and sources of legislation.

[142] An ANBI is a Public Benefit Organisation. To qualify with the Tax and Customs Administration, PBOs must meet a range of requirements (e.g. 90% of the organisation's activities must focus on the general good; www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/bijzondere_regelingen/goede_doelen/algemeen_nut_beogende_instellingen/wat_is_een_anbi.

[143] See the bibliography for official titles and sources of legislation.

[144] See the bibliography for official titles and sources of legislation.

the UBOs of corporate and other legal entities. This UBO information is expected to form part of the commercial register.

Other instruments

- *General terms and conditions of banks*. The general terms and conditions of banks regulate the interaction between banks and their clients, stipulating the rights and responsibilities of both parties. All members of the Dutch Banking Association (NVB) use the same general terms and conditions.[145] During the expert meeting, to help explicate the role played by general banking terms and conditions in preventing and combating money laundering, it was pointed out that they may be used by banks to refuse clients if there is any reason to do so. If a bank suspects a client of money-laundering practices, it may not legally share this with other banks due to privacy legislation.
- *Incident referral protocol (ERA register).* The External Referral Application (ERA) is the joint fraud prevention system run by the NVB and the Association of Financing companies in the Netherlands (VFN), which interconnects the fraud registers of the member organisations. The ERA register may be shared among NVB member banks. During the expert meeting, it was pointed out that banks may enter the details of persons or legal entities in the register who are guilty of fraud or otherwise constitute a risk. The relevant banks can check whether new clients are listed in the register, allowing them to refuse services to fraudulent parties.

5.3 Resilience of policy instruments

In the second expert meeting, the participants were asked to assess the extent to which the available policy instruments and their implementation in practice are effective in combating the ten identified risks. Fifteen experts were present at the meeting.[146]

5.3.1 Determining the key policy instruments for each risk

The available policy instruments were analysed in order to establish their effectiveness against each of the risks. To do so, an overview of the various relevant elements comprising the range of available policy instruments was created. As inspiration, the experts received a list of national policy instruments that help limit the opportunities for money laundering. This list included the Money Laundering and Terrorist Financing Prevention Act (Wwft), the Financial Supervision Act (Wft), the Trust and Company Service Providers (Supervision) Act (Wtt) and the Dutch Penal Code (WvS). For each risk, the experts were asked to supplement the list with other relevant policy instruments, including those with are set up on other levels. This resulted in the addition of European and other national, municipal, sectoral, branch/organisation-based instruments. For each risk, the experts were given 100 points to distribute across the entire range of instruments to indicate the extent to which each instrument contributes to preventing and/or combating that particular money-laundering risk.

Table 5.1 shows the key policy instruments per risk according to the experts, taking into account both their intended purpose and their implementation. The table shows the instruments that were awarded at least 10 points (out of 100) by experts. They

[145] www.ing.nl/de-ing/algemenebankvoorwaarden/index.html.

[146] See Appendix 3 for a list of the organisations represented in the second expert meeting.

therefore named more policy instruments than are listed here, however the remainder received fewer than 10 points. Appendix 7 presents all of the individual policy instruments and scores listed for each risk.

According to the experts, the Wwft plays an extremely significant role in preventing all ten risks. The WvS was deemed relatively very important for combating eight of the ten risks, and tax legislation for seven of the risks. The Wft was awarded ten or more points for five of the risks.

Table 5.1 Key policy instruments (10 points or more) per risk

Risks	Policy instruments (points given in brackets)
Money laundering via financial institutions (especially banks)	– Money Laundering and Terrorist Financing Prevention Act (Wwft, 33) – Financial Supervision Act (Wft, 20) – Dutch Penal Code (WvS, 11)
Money laundering via payment service providers	– Money Laundering and Terrorist Financing Prevention Act (Wwft, 38) – Financial Supervision Act (Wft, 27) – Dutch Penal Code (WvS, 13)
Money laundering via trust offices	– Trust and Company Service Providers (Supervision) Act (Wtt, 32) – Money Laundering and Terrorist Financing Prevention Act (Wwft, 28) – Tax legislation (14)
Money laundering via offshore firms	– Money Laundering and Terrorist Financing Prevention Act (Wwft, 30) – Tax legislation (15) – International treaties (15) – Trust and Company Service Providers (Supervision) Act (Wtt, 11) – Dutch Penal Code (WvS, 11)
Money laundering constructions to conceal actual value	– Money Laundering and Terrorist Financing Prevention Act (Wwft, 30) – Tax legislation (21) – Dutch Penal Code (WvS, 17)
Trade-Based Money Laundering	– Specific, nationally-applicable EU legislation (30) – Tax legislation (23) – Money Laundering and Terrorist Financing Prevention Act (Wwft, 22) – Dutch Penal Code (WvS, 11)
Money laundering via fiscally driven/complex corporate structures	– Tax legislation (29) – Money Laundering and Terrorist Financing Prevention Act (Wwft, 28) – Trust and Company Service Providers (Supervision) Act (Wtt, 12) – Commercial Register Act, incl. UBO (10)
Money laundering via virtual currencies	– Money Laundering and Terrorist Financing Prevention Act (Wwft, 39) – Dutch Penal Code (WvS, 20) – Financial Supervision Act (Wft, 17) – General terms and conditions of banks (12)
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	– Money Laundering and Terrorist Financing Prevention Act (Wwft, 25) – Dutch Penal Code (WvS, 24) – Specific, nationally-applicable EU legislation (21) – Financial Supervision Act (Wft, 15) – Tax legislation (10)
Money laundering via national and international investment structures for value transfer	– Money Laundering and Terrorist Financing Prevention Act (Wwft, 23) – Tax legislation (22) – Financial Supervision Act (Wft, 17) – Dutch Penal Code (WvS, 14)

During the expert meeting and interviews, two general points were raised that may impact the resilience of policy instruments in preventing and combating money laundering.

According to the experts, the implementation of the policy instruments depends in part on the available capacity at the organisations responsible for preventing and combating money laundering. Capacity is one of the deciding factors in the development of anti-money laundering policy. One of the supervisory bodies stated, for example, that their capacity influences how they perform their sector inspections, i.e. based on indications rather than a sector-wide approach. Furthermore, low capacity combined with performance requirements can result in a focus on straight forward money-laundering practices that are relatively easy to detect, since they offer 'fast results'.[147] This focus can be at the expense of preventing and combating the more complex forms of money laundering that are harder to detect (but which may nonetheless have a more significant impact). These more complex cases requiring greater capacity carry the risk of producing results that are limited or indirect (or none at all). A pronounced focus on straight forward cases can thwart the growth of knowledge required for working with a risk-based approach, which is of particular relevance to newly identified risks or the risks inherent to complex cases.

Exchange of information among supervisory bodies, FIU Netherlands, the Tax and Customs Administration, the Police, the Public Prosecution Service and banks is critical in preventing and combating money laundering. To a varying extent, all of these parties possess data that are potentially useful in detecting and combating (potential) money-laundering practices. Although various partnerships have been set up for data and information-exchange purposes, such as the iCOV, AMLC and the RIECs, not all information can be shared between one another due to privacy legislation (such as the Personal Data Protection Act[148] and European privacy legislation) and supervisory confidentiality[149]. During the interviews and meetings, the experts regarded information and data-sharing limitations between organisations as a sticking point in preventing and combating money laundering. A Data Processing Partnerships Act is currently being drafted, with the aim of eliminating sticking points which may occur.

While this is a concern in the Netherlands, ensuring information and data exchange internationally is even more difficult. The interviews and expert meetings revealed that aspects such as differing legal frameworks and the resulting (occasional) incompatibilities between money-laundering definitions hamper information and data-sharing in practice. However, initiatives are currently being developed to make it easier for supervisory bodies, investigative and law enforcement authorities to share information and data internationally.

[147] 'Decide' came to the same conclusion in 2015 in the initial version of its anti-money laundering policy monitor. See also Van der Knoop & Rollingswier (2015, p. 69, 74).

[148] See the bibliography for official titles and sources of legislation. On 25 May 2018, the Personal Data Protection Act will be replaced by new Europe-wide privacy legislation: the General Data Protection Regulation (GDPR).

[149] Supervisory confidentiality is a fundamental principle of the Financial Supervision Act and the Trust Offices Supervision Act, and exceptions are only possible in certain exhaustibly listed cases.

5.3.2 *Resilience of the entire range of policy instruments*

The resilience of the available policy instruments for preventing and combating money laundering was measured twice. At the start of the second expert meeting, the participants made an initial judgement of the resilience of the *entire range* of policy instruments in combating money laundering. They were given no assistance e.g. criteria in doing so, however they did take both the intended purpose and the implementation of the instruments into consideration. For each risk, the experts estimated the resilience of the range of policy instruments on a scale from 0-100%. The score was intended to reflect the extent to which the entire range of available policy instruments combated the specific money-laundering risk.

The second judgement was made following the discussion on the relative contribution made by *each individual policy instrument* for each risk, the results of which were presented in the previous section. This discussion (run according to the Delphi method) could have resulted in the experts changing their original judgements regarding the resilience of the instruments. The second round showed only limited differences, however; the average resilience of the entire range of policy instruments per risk remained virtually unchanged.[150] For this reason, the table below presents only data from the second estimation. Analogous to the risk assessments in Section 4, the resilience figures are clustered into bracketed ranges. The exact figures on the two different measurements can be found in Appendix 7.

Table 5.2 Average resilience of the entire range of policy instruments per risk

Risk	Type of risk	Resilience (on a scale of 0-100%)
Money laundering via financial institutions (especially banks)	Money-laundering channel	41-50%
Money laundering via payment service providers	Money-laundering channel	
Money laundering via trust offices	Money-laundering channel	31-40%
Money laundering via fiscally driven/complex corporate structures	Money-laundering method	
Money laundering via national and international investment structures for value transfer	Money-laundering method	
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	Money-laundering method	21-30%
Money laundering constructions to conceal actual value	Money-laundering method	
Money laundering via offshore firms	Money-laundering method	
Trade-Based Money Laundering	Money-laundering method	
Money laundering via virtual currencies	Money-laundering method	11-20%
Average resilience		32%

According to the experts, nearly half of the risks of money laundering via financial institutions (banks in particular) and payment service providers are mitigated by the available policy instruments. The lowest resilience score was given to the instruments for preventing and combating money laundering via virtual currencies. The entire range of policy instruments reduces the main ten money-laundering-related risks on average by approximately one-third.

[150] The estimated resilience of seven of the ten risks did turn out to be lower after discussing the instruments' effectiveness per risk and the ensuing plenary discussions, however.

The lowest resilience was allocated to (1) money-laundering methods which are not regulated, (2) methods including an international component, and (3) relatively anonymous methods. All three of these aspects would seem to apply to virtual currencies, which may explain the low resilience score. The same applies to a lesser extent to TBML and offshore companies, as well as physical cash transport and money laundering constructions to conceal actual value. By contrast, the existing policy instruments score higher on methods applied in regulated environments.

6 Conclusions

This section begins by presenting the key results of this first NRA on money laundering, which are described using the answers to the research questions. This is followed by an evaluation of the NRA, highlighting both the strengths and weaknesses of the research methodology applied. Finally, this section discusses some lessons learned that may be useful in designing the next NRA.

6.1 Answers to research questions

Research question 1: What context variables make the Netherlands vulnerable to money laundering?

For the purposes of this first NRA, a context analysis was conducted that examined circumstances in the Netherlands that are believed to be of influence in regard to the prevention of money laundering, taking economic, geographic and demographic features of the Netherlands into account, along with the criminological landscape. During this context analysis, earlier studies were taken into account which indicate factors that may make the Netherlands vulnerable to money laundering. According to several studies the Netherlands is vulnerable to money laundering due to its open, commerce-oriented economy, its vast and internationally oriented financial sector and the scale of criminal income from fraud (including tax fraud) and drug-related crime. These are the conclusions issued by the FATF in its Mutual Evaluation Report of the Netherlands of 2011. These results were confirmed by research and publications by other institutes, including publications recently released in 2017.
In addition, the results of the Transcrime project IARM indicate that the Dutch gambling, catering, and art and entertainment sectors are vulnerable to money laundering due to the involvement of organised crime, the occurrence of fraudulent activity, the widespread use of cash in these sectors and lack of clarity regarding ultimate beneficial owners.[151] This latter aspect was also mentioned in a recent report by Transparency International Netherlands, in which the Netherlands is considered lagging behind with regard to the central registration of ultimate beneficial owners.[152]
However, the Netherlands also has characteristics that make it less vulnerable to money laundering in comparison to other countries. For example, the extent of organised crime in the Netherlands is relatively small and there are very few black markets for smuggled goods.

Research question 2: Which ten money-laundering risks can be deemed to present the greatest potential risk, in view of the Dutch context?

The ten main risks in terms of their potential impact are displayed in Table 6.1. The risks are clustered into bracketed ranges since the maximum and the minimum risk levels of the identified risks are relatively close to each other, the difference between a number of risk levels was relatively small and not all estimates by the experts were or could fully be substantiated. Money laundering via financial institutions was assessed as having the greatest potential impact. Experts attributed the highest potential risk level to the misuse of bank services due to the vast amounts of money involved in the financial sector.

[151] Savona & Riccardi (2017).

[152] Streiff & Scheltema Beduin (2017).

Table 6.1 The experts' ten main money-laundering-related risks*

Risk	Potential risk level (On a scale of 0-100)
Money laundering via financial institutions (especially banks)	71-75
Money laundering via payment service providers Money laundering via trust offices Money laundering via offshore firms	61-70
Money laundering constructions to conceal actual value Trade-Based Money Laundering Money laundering via fiscally driven/complex corporate structures Money laundering via virtual currencies Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise) Money laundering via national and international investment structures for value transfer	55-60

Research question 3: Which risks have not yet been identified in the Netherlands, but could be relevant in the future? How can this situation be clarified?

During the expert meetings for this first NRA, the attention focused on money-laundering risks that the participants believe to exist *at this current moment*. With regard to possible 'future risks', only limited information was obtained during the meetings were is was touched upon briefly and the in-depth interviews that followed. One possible future risk that was mentioned relates to the 'new economy', reflecting global technological changes in fields as internet and telecom. The introduction of new (technologal) products and services creates new opportunities for criminals to launder their illicit proceeds.

Definitely one of the ten risks identified during the expert meetings, money laundering via virtual currencies, is 'future-oriented' in nature. However, since experts have as yet barely encountered this risk in their everyday professional practice, the substantiation of this risk leaves something to be desired. At the same time it was considered that despite the considerable fluctuations in value of several virtual currency denominations such as bitcoin, ethereum and monero in the last year, the overall trend is a vast and steady value increase of 'crypto currencies'.[153] The resulting public attention combined with the (as yet) limited resilience of the instruments to mitigate these risks meant that virtual currencies were identified as a possible future money-laundering risk.

Research question 4: What policy instruments are available in the Netherlands to combat the risks?

Dutch policy to prevent and combat money laundering is based on the recommendations of the Financial Action Task Force (FATF) and the relevant regulatory framework from the European Union. The available policy instruments to prevent and combat money laundering also include all relevant instruments stemming from national, international and municipal legislation and regulations within individual entities. These include:

[153] Between 18 September 2016 and 17 September 2017, the value of bitcoin, ethereum and monero rose by 583%, 1892% and 974% respectively. Source: www.coinmarket.cap.

National legislation
- The Money Laundering and Terrorist Financing Prevention Act (Wwft)
- The Financial Supervision Act (Wft)
- The Dutch Penal Code (WvS)
- The Trust and Company Service Providers (Supervision) Act (Wtt)
- Tax legislation
- The Public Administration Probity Screening Act (*Wet Bibob*)
- Commercial Register Act 2007

European legislation
- EU Anti-Money Laundering Directive
- EU Regulation on Controls of Cash
- The revised Wire Transfer Regulation (WTR2)

Other instruments
- General terms and conditions of banks
- External Referral Application (ERA)

Research question 5: To what extent can the existing range of policy instruments be expected to effectively combat the risks?

The response to research question 4 above reveals the extensive arsenal of policy instruments available for combating money laundering. The experts indicated that in principle, they are positive about the instruments at their disposal; according to them no important elements are missing. However, this does not mean that they believe the available policy instruments can entirely eliminate the risks of money laundering. During an expert meeting, experts were invited to consider to what extent the identified risks would be mitigated by the application of the policy instruments. They estimated that the instruments would reduce the money-laundering risks identified in this NRA on average by around one-third (see Table 6.2).

Table 6.2 Average resilience of the entire range of policy instruments per risk

Risk	Type of risk	Resilience (on a scale of 0-100%)
Money laundering via financial institutions (especially banks)	Money-laundering channel	41-50%
Money laundering via payment service providers	Money-laundering channel	
Money laundering via trust offices	Money-laundering channel	31-40%
Money laundering via fiscally driven/complex corporate structures	Money-laundering method	
Money laundering via national and international investment structures for value transfer.	Money-laundering method	
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	Money-laundering method	21-30%
Money laundering constructions to conceal actual value	Money-laundering method	
Money laundering via offshore firms	Money-laundering method	
Trade-Based Money Laundering	Money-laundering method	
Money laundering via virtual currencies	Money-laundering method	11-20%
Average resilience		32%

The resilience of the policy instruments is relatively highest for the risk of 'money laundering via financial institutions (especially banks)' and 'money laundering via payment service providers' since these sectors are regulated, anonymous transactions are in principle prohibited, and are addressed effectively in the Netherlands.

Research question 6: Which risks do the Dutch policy instruments fail to address, and why? What measures could resolve this situation, and to what extent are they feasible?

The experts noted that the available policy instruments (and the implementation thereof) to prevent and/or combat money-laundering risks with an international component have its limitations in an international environment, for example in Trade-Based Money Laundering and money laundering via offshore firms. The low resilience of the policy instruments regarding such risks is also evident in Table 6.2 above. For the effective prevention and combat of money laundering with a strong international component, international collaboration and data sharing between supervisory, investigative and law enforcement authorities is key. However, such international collaboration appears difficult to realise in practice because of different definitions of money laundering and different judicial systems. The experts also believe the available policy instruments are insufficient to effectively mitigate money-laundering risks involving unlicensed (financial) entities and service providers, for example, unlicensed payment service providers or underground banking. Furthermore, there is a relatively low level of resilience against methods allowing anonymous transactions, such as money laundering via virtual currencies and underground banking. The nature and methodology of virtual currencies are still evolving, hence, the risks have not yet been fully crystallised. For this type of risk, the experts believe that the existing policy instruments offer only limited resilience.

Research question 7: Which risks remain after implementation of the policy instruments? How serious are the remaining risks relative to one another?

The study looked at the resilience of the policy instruments and their implementation in practice (see also the response to research question 5 above). A large proportion of the ten identified risks cannot be mitigated by the available policy instruments, and all of them remain risks to a greater or lesser extent. The policy instruments reduce two of the risks by nearly half: 'money laundering via financial institutions (especially banks)' and 'money laundering via payment service providers'. The resilience of the available policy instruments is extremely limited when it comes to 'money laundering via virtual currencies', as these currencies are unregulated, relatively anonymous and international in character. The resilience of the policy instruments decreases the more these aspects (anonymity, no regulation and international aspects) come into play.

Research question 8: What quantitative data could be used in a subsequent NRA to create an overview of money-laundering risks?

The e-mail questionnaire produced little information, due in part to the limited response by the experts invited, and partly due to the lack of detail in the respondents' answers.

Two money-laundering research projects that are currently underway will be complete when the next NRA is produced: the 'Anti-money laundering policy monitor' and a study on the 'Nature and scope of criminal spending'. The results of these studies are expected to be of use in the next NRA.

Research question 9: What are the lessons learned that could be applied to subsequent NRAs?
The following sections respond in detail to this research question. First of all, the strengths and weaknesses of this NRA are highlighted, followed by a description of several of the lessons learned that could potentially be of use in producing the next NRAs.

6.2 Evaluation of the first NRA

Section 2 gave a comprehensive description of the methodology used in this first NRA. In short, it involved the following:

- A context analysis that depicts specific characteristics of the Netherlands that are believed to be of influence in regard to the prevalence of money laundering. For the purposes of this context analysis, a literature study was conducted.
- In order to identify threats related to money laundering, the following activities were conducted:
  - An extensive literature study (examining six foreign NRAs, the European Supranational Risk Assessment, the National Threat Assessment for Organised Crime 2017-2021 and other relevant reports);
  - An e-mail questionnaire was sent to representatives of expert organisations;
  - Interviews were held with academics and representatives of expert organisations.
- A first expert meeting was organised in which representatives of the expert organisations identified the greatest money-laundering risks in terms of their potential impact. They also estimated the potential impact of these risks.
- After the first expert meeting, an e-mail questionnaire was sent to the participants to inquire which data reflect the prevalence of the ten identified risks. In the questionnaire, the experts were also asked if these data were available (to third parties) and which other – now unavailable – data exist that reflect the prevalence of the ten identified risks.
- In a second expert meeting, representatives of expert organisations assessed the resilience of the available policy instruments designed to prevent or combat the ten risks.
- In the final stage of the research, a series of validation interviews were conducted with key experts with the primary purpose of examining to what extent they recognise the identified risks and whether any significant risks have been overlooked.

It can be seen from the above methodology that this initial NRA is qualitative in nature, and is predominantly based on experts' opinions and estimates.

Strengths of the first NRA
In terms of its implementation, this first NRA has a number of strong points.

- *Close collaboration with the sector.* One general strength of this first NRA is the fact that all organisations involved in preventing and combating money laundering in various ways were involved in the study at one or several stages. These organisations – each with their own field of expertise – represent the combined experience in the Netherlands in the field of preventing and combating money laundering.
- *Transparent data collection.* The (qualitative) data used in this initial NRA were collected in a transparent manner, thereby also increasing the study's reproducibility.

- *Great added value from Group Discussion Rooms (GDRs).* Firstly, the GDRs acted as a catalyst: the experts entered their opinions and estimates into a digital system, the aggregated outcomes of which were then presented in real time. Compared to 'traditional' meetings this not only saved time, but also afforded greater opportunities for deepening the results through plenary discussion. The frequent variation between group discussions and answering questions or giving opinions/estimates on a laptop also kept the level of active participation by experts high throughout the entire meeting. Thirdly, the figures on the potential risks and resilience were determined using the information supplied by the experts through the GDR environment, ensuring that all relevant perspectives were represented in the final results and reducing or eliminating the effects of a potential sticking point arising from an expert-oriented approach i.e. opinions being influenced by (organisational) interests. Lastly, the use of GDR also facilitated data collection.
- *The structuring effect of the Multi-Criteria Analysis (MCA).* The MCA was conducted within the GDR environment, and helped to structure the meeting itself and the collection of data, while also giving transparency to the results and the way they were generated. Under the MCA, the experts used predetermined criteria to evaluate the potential impact of each of the money-laundering risks. This method made it less likely for experts to be swayed by their possible organisational interests when evaluating the severity of the risks.
- *The Delphi method: a key component in risk identification.* One application of the Delphi method was in risk identification: experts were given two opportunities to put forward what they believed were the greatest money-laundering risks. The experts altered their opinions so that 'money laundering via virtual currencies', which had originally been left off the list of the greatest threats in round one, returned to the list after hearing the arguments during the group discussion. This was a significant development, as the second expert meeting revealed that the existing policy instruments are ill-equipped to address that particular risk.
- *Good preparation of expert meetings is vital.* A script was drawn up in advance to help structure the expert meetings. To prevent different interpretations of questions and concepts during the expert meetings, information on the applicable definitions and MCA criteria was drawn up beforehand and sent to the experts in order to get everyone 'on the same page'. The participants also received a document containing a summary of the context analysis before the expert meeting. Lastly, handouts were issued during both expert meetings, containing information on the MCA definitions and criteria, which were also discussed as a group. A well-known pitfall of GDR is that of 'groupthink', which was avoided here as much as possible through the appointment of a professional, independent chairperson from APE Public Economics, whose task was to encourage the experts to substantiate and explain the opinions they had submitted to the GDR environment, and to present case studies.
- *Extensive list of threats.* The various research activities in the early stages produced an extensive longlist of money-laundering threats. During the first expert meeting, it became clear that the proposed longlist was almost exhaustive; the experts made only a few additions.
- *Validation of the NRA results.* During the final stages of the NRA, interviews were held with key experts (from the Police, AMLC and the ministries of Finance and Security and Justice). The key question for the Police and AMLC concerned the extent to which they could validate the identified risks. With the ministry representatives, the list was discussed in a more general sense. This validation process confirmed the relevance of all the identified risks, and also the fact that according to the interviewees no significant risks were missing from the list.

Areas of attention

The execution of this first NRA also revealed some areas of attention , most of which concern the predominantly qualitative character of the research methodology.
The NRA is based primarily on the opinions and estimates of representatives from supervisory, investigative and law enforcement authorities and the sector/umbrella organisations of obliged entities. This means that the identification of the risks, estimation of their potential impact and assessment of the resilience of policy instruments all include a subjective element, and may be reliant (wholly or in part) on individual perceptions and/or personal judgements.
During the expert meetings, it seemed that the levels of knowledge varied: not all experts demonstrated the same degree of expertise in all topics discussed, and not all opinions could be satisfactorily substantiated. This could be due to the variation in the experts' involvement in preventing and combating money laundering. Each expert having its own specialist field meant that the participants had more knowledge of some risks and less of others. The level of general knowledge among the participants also varied. No correction e.g. weighting was applied for this difference in expertise, as no objective grounds were found for determining weights. Moreover, there was no single participant with full knowledge of the entire sector or a complete understanding of all money-laundering risks and/or the resilience of policy instruments.
Despite some experts' extensive knowledge in the field or parts thereof, it was difficult for them to make a substantiated quantitative judgement of the prevalence and impact of the money-laundering risks, and the resilience of the instruments. To limit this effect, during the plenary session the experts were asked to present any data or specific examples they had of risks and policy instruments. They were also asked *not* to make a quantitative estimate of the potential impact of any risk or the resilience of policy instruments if, in their view, they did not have the necessary knowledge to do so. For most risks there was at least one expert who did not make a resilience estimate, and there was one risk for which six of the fifteen experts declined to make an estimate.
Lastly, it proved difficult to get *all* of the relevant expert organisations to participate in the expert meetings – not all of them accepted the invitation to take part, and some who initially did accept were unable to attend. Some expert organisations were represented at one meeting but not the other. Because it is conceivable that some relevant knowledge on the risks was therefore missing during the expert meetings, validation interviews were held afterwards with the expert organisations who were not represented at one or both meetings (see also the previous section).

6.3 Lessons learned for the next NRA

This section outlines a number of lessons learned that should be taken into account during the implementation of subsequent NRAs.

More quantitative research results

In subsequent NRAs, the research methodology should be more data-oriented, as this will reduce the risk of possible (partly) subjective expert opinions and this should be contributing to an increased reliability of the results.
For future expert meetings, quantitative data should be incorporated as much as possible to ‘synchronise’ the experts' frames of reference even more. The results of the two WODC studies currently being conducted, the ‘Anti-Money Laundering Monitor’ and a study on the ‘Nature and scope of criminal spending’, may be of use in this respect, and are expected to be available when the next NRA is conducted.

Ideally, the longlist of threats should to the largest extent possible be based on existing data indicating the prevalence and potential impact of the threats. Finally, greater substantiation should be given by experts for the selection of the (ten) main risks, preferably backed up with data.
There are two points to note, however. Firstly, in some cases data regarding risk prevalence and potential risk impact are simply missing; in other cases these data may be available from certain organisations, but cannot be used for the NRA due to privacy legislation or supervisory confidentiality. Secondly, the extent to which experts are able or permitted to support their arguments using hard data is still uncertain, as this proved very difficult for them during this initial NRA.

Greater substantiation and depth
The expert meetings were characterized by a full programme. Although the scripts helped to get through everything without running overtime too much, there was not always sufficient time devoted to substantiating the experts' judgements or analysing case studies. This, combined with the fact that some experts were not always in a position to disclose what they knew or were missing knowledge in certain areas, meant that certain parts of the present NRA are more general in nature.

Maintaining the GDR approach
Even if the next NRA is more data-oriented, the qualitative opinions of experts will still play a key role. After all, expert opinions will always be important in the substantiation and interpretation of quantitative data, as well as for obtaining information on topics for which no quantitative data is (currently) available. Some data on risks are simply missing, or cannot be made publicly available by the relevant organisation. Given the considerable effectiveness of the GDR in conducting this initial NRA, the use of it for the following NRAs is recommended. However, it will be useful to consider whether the presentation of (quantitative) judgement' questions to the experts can be simplified.
As the section above pointed out, it proved difficult for some experts - despite their specialist knowledge in (certain) areas - to satisfactorily substantiate their quantitative judgements regarding the prevalence and potential impact of money-laundering risks and the resilience of policy instruments.
No major changes to the GDR structure are required. The number and origins of the participants, around 15, representing all relevant organisations involved, proved ideal for raising and discussing a wide variety of topics. One possible idea would be to extend the length of the meetings e.g. to 4 or 5 hours, providing extra time for more in-depth exploration of some topics. The expert meetings held for this first NRA sometimes lacked the time necessary for discussing all topics to the same extent, or for checking the experts' opinions. Extra time would have also allowed for more in-depth discussion of case examples of money-laundering risks, as well as the potential side-effects or counterproductive elements of policy. The potential negative effects of lengthening the meetings should also be noted, however. A break would be required in order for the experts to maintain concentration, and a longer session could reduce attendance (as longer meetings place greater demands on experts' agendas).

MCA criteria review
The potential impact of the ten main risks was determined using an MCA, which included seven criteria. These were distilled from the FATF Guidance overview on the consequences and effects of money laundering, an evaluation of the criteria raised during the expert interviews, and a discussion on the criteria by the advisory

committee. In practice, some of the criteria turned out to be not very distinctive, as they were rated above-average on all risks by all experts, mainly 'the degree to which regular society is interwoven with the criminal underworld' and 'the manifestation or facilitation of crime or terrorist activities'.
A comparison of the rankings from the frequency-based and MCA-based approaches showed that seven of the ten risks were ranked in the same order, and that no risk shifted by more than two places. Although this cannot be called a completely independent validation assessment, in conjunction with the subsequent validation interviews it does give some confidence in the MCA results. Nevertheless, the criteria should be critically reviewed for the following NRA, particularly those providing little differentiation.

More limited use of the Delphi method
Although it has already been mentioned above that the Delphi method proved useful in the identification of money-laundering risks, it had little to offer in terms of evaluating the resilience of policy instruments: there was very little difference between the initial resilience scores and those that emerged following the group discussion. In the next NRA, a single resilience evaluation will suffice, to occur after the group discussion. The time thus saved can be spent on more in-depth group discussions and on the presentation of case studies to underpin the relative importance of the money-laundering risks.

Bibliography

Blauw (2016). Crimineel vermogen in belastingparadijs is onzichtbaar. Blauw, 30 januari 2016(1).

Boerman, F., Grapendal, M., Nieuwenhuis, F., & Stoffers, E. (2017). Nationaal Dreigingsbeeld 2017: Georganiseerde criminaliteit. Zoetermeer: Politie, Dienst Landelijke Informatieorganisatie.

Bouman, M. (2016). Export van diensten neemt de Nederlandse economie op sleeptouw. Financieel Dagblad, 13 mei 2016.

Central Intelligence Agency (2017). The world factbook. Washington, D.C: CIA.

Department of State. Bureau for International Narcotics and Law Enforcement Affairs. (2017a). 2016 International Narcotics Control Strategy Report Volume I: Drug and chemical control. Z.pl.: United States Department of State.

Department of State. Bureau for International Narcotics and Law Enforcement Affairs (2017b). 2016 International Narcotics Control Strategy Report Volume II. Money laundering and financial crimes. Z.pl.: United States Department of State.

Europese Commissie (2017). Supranational risk assessment of the money laundering and terrorist financing risks affecting the EU. Brussel: Europese Commissie.

EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) (2016). Rapport over de drugsmarkten in de EU. Strategisch overzicht 2016. Den Haag: Europol.

EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) (2017). Netherlands country overview. Den Haag: Europol.

Europees Parlement (2015). Economic, social and territorial situation of the Netherlands: In-depth analysis. Brussel: Europees Parlement. IP/B/REGI/INT/2015-01 February 2015, PE 540.353 EN.

Europees Parlement (2016). Virtual currencies: Challenges following their introduction: Briefing March 2016. Brussel: Europees Parlement.

Europol (2015). Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering. Den Haag: Europol.

FATF (2011). Anti-money laundering and combating the financing of terrorism: The Netherlands: Mutual Evaluation Report. Parijs: FATF.

FATF (2012). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations. Parijs: FATF.

FATF (2013a). Guidance national money laundering and terrorist financing risk assessment. Parijs: FATF.

FATF (2013b). Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AMF/CFT systems. Parijs: FATF.

FATF (2014). Mutual evaluation of the Netherlands: 2nd follow-up report. Parijs: FATF.

FIU-Nederland (z.j.). Informatieblad 'Hoe meld ik een ABC-transactie aan FIU-Nederland'. Zoetermeer: FIU-Nederland.

International Monetary Fund (2017). Kingdom of the Netherlands-Netherlands : Financial system stability assessment. Washington, D.C.: International Monetary Fund, Monetary and Capital Markets Department. IMF Country Report No. 17/79.

ISO 31000:2009 (2009a). Risk management: Principles and guidelines. Genève: International Organization for Standardization.
ISO/IEC 31010:2009 (2009b). Risk management: Risk assessment techniques. Genève: International Organization for Standardization.
Kerste, M., Baarsma, B., Weda, J., Rosenboom, N., Rougoor, W., & Risseeuw, P. (2013). Uit de schaduw van het bankwezen: Feiten en cijfers over bijzondere financiële instellingen en het schaduwbankwezen. Amsterdam: SEO Economisch Onderzoek.
Knoop, J. van der, & Rollingswier, R. (2015). De bestrijding van witwassen, beschrij-ving en effectiviteit 2010-2013: Startversie monitor anti-witwasbeleid. Den Haag: Dutch Group – Decide.
Knoop, J. van der (2017). Risico's van witwassen en terrorismefinanciering in de kansspelsector: Quickscan. Den Haag: Decision Support.
Koningsveld, T.J. van (2008). Witwassen: De fasen van het witwasproces getoetst. Tijdschrift voor Onderneming en Financiering, 4, 88-104.
Kruisbergen, E.W. , Bunt, H.G. van de , Kleemans, E.R. , Kouwenberg, R.F., Huisman, K., Meerts, C.A., & Jong, D. de (2012). Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Crimi-naliteit. Den Haag: Boom Lemma. Onderzoek en beleid 306.
Laar, M. van, & Ooyen-Houben, M. (red) (2016). Nationale Drugs Monitor 2016. Utrecht/Den Haag: Trimbos-instituut/WODC.
Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2016). Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware. Den Haag: Boom criminologie. Onderzoek en beleid 319.
Savona, E.U., & Riccardi, M. (red.) (2017). Assessing the risk of money laundering in Europe: Final report of Project IARM. Milaan: Transcrime – Università Cattolica del Sacro Cuore.
Soudijn, M., & Akse, Th. (2012). Witwassen Criminaliteitsbeeldanalyse 2012. Driebergen: KLPD.
Streiff, F., & Scheltema Beduin, A. (2017). Behind the scenes: Beneficial ownership transparency in the Netherlands. Z.pl.: Transparancy International Nederland.
Transparency International (2017). Corruption Perceptions Index 2016. Berlijn. Z.uitg.
Unger, B. (2006). De omvang en het effect van witwassen. Justitiële verkenningen, 32(2), 21-33.
Unger, B. (2013). Money laundering regulation: From Al Capone to Al Qaeda. In B. Unger & D. van der Linde (red.), Research handbook on money laundering (pp. 19-32). Cheltenham, Engeland: Edward Elgar.
Unger, B., H. Addink, J. Walker, J. Ferwerda, M. van den Broek, & I. Deleanu (2013). Project 'ECOLEF': The economic and legal effectiveness of antimoney laundering and combating terrorist financing policy: Final report. Project funded by the European Commission DG Home Affairs JLS/2009/ISEC/AG/087. Utrecht: Utrecht University.
Unger, B., Rawlings, G., Busuioc, M., Ferwerda, J., Siegel, M., Kruijf, W. de, & Wokke, K. (2006). The amounts and the effects of money laundering. Den Haag: Ministerie van Financiën.
Veen, H.C.J. van der, & Ferwerda, J. (2016). Verkenning methoden en data National Risk Assessment Witwassen en Terrorismefinanciering. Den Haag: WODC. Cahier 2016-12.

Verenigde Betaaldienstverleners Nederland (z.j.). Betaaldienstverleners en Elektronisch Geldinstellingen. Wat zijn dat?. Z.pl.: Z.uitg.
World Economic Forum (2016). Global Competitiveness Report 2016-2017. Genève: World Economic Forum.

Other sources

NRA's

Department of Finance Canada (2015). Assessment of inherent risks of money laundering and terrorist financing in Canada. Z.pl.: Department of Finance Canada.

Department of Finance, & Department of Justice and Equality (2016). National risk assessment for Ireland: Money laundering and terrorist financing. Z.pl.: Department of Finance, Department of Justice and Equality.

Department of the Treasury (2015). National money aundering risk assessment. Washington, DC: Department of the Treasury.

Financial Security Committee (2014). Analysis of Italy's national money laundering and terrorist financing risks: Methodology.Rome: Ministerio dell'Economia e delle Finanze, Financial Security CommitteeUitgever.

HM Treasury, & Home Office (2015). UK national risk assessment of money laundering and terrorist financing. Z.pl.: HM Treasury / Home Office.

Swedish Companies Registration Office, The Swedish National Council for Crime Prevention, The Swedish Economic Crime Authority, The Swedish Estate Agents Inspectorate, Finansinspektionen (the Swedish financial supervisory authority), The Swedish Enforcement Authority, The Swedish Gambling Authority, Stockholm County Administrative Board, Västra Götaland County Administrative Board, Skåne County Administrative Board, The Swedish Supervisory Board of Public Accountants, The Swedish National Police Board, The Swedish National Tax Board, The Swedish Bar Association, The Swedish Security Service, Swedish Customs, and The Swedish Prosecution Authority (2013). Anti-Money Laundering. A National Risk Assessment. Joint report.

Websites

• https://data.oecd.org.
• http://eur-lex.europa.eu.
• http://ec.europa.eu/eurostat.
• https://fd.nl.
• http://juridischactueel.nl.
• https://tradingeconomics.com.
• http://wetten.overheid.nl.
• www.afm.nl.
• www.advocatie.nl.
• www.banken.nl.
• www.belastingdienst.nl.
• www.bijzonderstrafrecht.nl.
• www.burojansen.nl.
• www.cbs.nl.
• www.coinmarket.cap.
• www.dnb.nl.
• www.fatf-gafi.org.
• www.ing.nl.
• www.om.nl.
• www.rijksoverheid.nl.
• www.toezicht.dnb.nl.

- www.topsectoren.nl.
- www.trouw.nl.
- www.volksgezondheidenzorg.info.

Sources of legislation

Title	Abbreviation	Location:	Website
The Money Laundering and Terrorist Financing Prevention Act	Wwft	Origin: *Bulletin of Acts and Decrees* 2008, 303 Entered into force: *Bulletin of Acts and Decrees* 2008, 304 Last amended by law on 11 August 2016, Bulletin of Acts and Decrees 2016, 297	http://wetten.overheid.nl/BWBR0024282/2016-08-11
Financial Supervision Act	Wft	Origin: *Bulletin of Acts and Decrees* 2006, 475 Entered into force: Bulletin of Acts and Decrees 2006, 664 Last amended by law on 1 September 2017, Bulletin of Acts and Decrees 2017, 174	http://wetten.overheid.nl/BWBR0020368/2017-09-01
Trust and Company Service Providers (Supervision) Act	Wtt	Origin: *Bulletin of Acts and Decrees* 2004, 9 Entered into force: Bulletin of Acts and Decrees 2004, 58 Last amended by law on 01 January 2015, Bulletin of Acts and Decrees 2014, 534	http://wetten.overheid.nl/BWBR0016189/2015-01-01
Dutch Penal Code	WvS	Origin: Bulletin of Acts and Decrees 1881, 35 Entered into force: Bulletin of Acts and Decrees 1886, 64 Last amended by law on 01 January 2015, Bulletin of Acts and Decrees 2017, 191	http://wetten.overheid.nl/BWBR0001854/2017-09-01
Public Administration Probity Screening Act	*Wet Bibob*	Origin: Bulletin of Acts and Decrees 2002, 347 Entered into force: Bulletin of Acts and Decrees 2002, 502 Last amended by law on 1 July 2016, Bulletin of Acts and Decrees 2016, 243	http://wetten.overheid.nl/BWBR0013798/2016-07-01
Data Protection Act	Wbp	Origin: Bulletin of Acts and Decrees 2000, 302 Entered into force: Bulletin of Acts and Decrees 2001, 337 Last amended by law on 01 July 2017, Bulletin of Acts and Decrees 2017, 279	http://wetten.overheid.nl/BWBR0011468/2017-07-01
Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the	Fourth EU Anti-Money Laundering Directive	PbEU 2015, L 141/73	http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015L0849&from=

Title	Abbreviation	Location:	Website
financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC			EN
Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006	Wire Transfer Regulation 2 (WTR2)	PbEU 2015, L 141/1	http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015R0847&from=EN
Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls on cash entering or leaving the Community	EU Regulation on Controls of Cash	PbEU 2005, L 309/9	http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32005R1889&from=NL
Proposal for a Regulation of the European Parliament and of the Council on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005	-	Com (2016) 825	http://eur-lex.europa.eu/resource.html?uri=cellar:4c6c5737-c8f5-11e6-ad7c-01aa75ed71a1.0008.02/DOC_1&format=PDF

Appendix 1 Members of the advisory committee

Chair	
Prof. W.F.M. Bams	Maastricht University, School of Business and Economics
Members	
J.C. Glimmerveen LLM	Ministry of Finance, Financial Markets, Institutional Policy and Integrity
E. Meijer LLM	Ministry of Finance, Financial Markets, Institutional Policy and Integrity
M. Rehorst LLM	Ministry of Security and Justice, Law Enforcement and Crime Fighting Department
Analyst	Ministry of Security and Justice, National Coordinator for Security and Counterterrorism
Dr J. van der Knoop	Decision Support
Dr J. Ferwerda	Utrecht University
D. Weggemans, MSc	Leiden University, Institute for Security and Global Affairs

Appendix 2 List of interviewees

In order to preserve the anonymity of the respondents, this list gives only the names of the organisations where they are employed. The number of interviewed employees is given for each organisation.

Organisation	No. of interviewees
Anti Money Laundering Centre	2 employees
Netherlands Authority for the Financial Markets	3 employees
Financial Supervision Office	2 employees
Wwft Supervision Office	2 employees
Dutch Central Bank	2 employees
Customs Netherlands	2 employees
FIU Netherlands	2 employees
The Hague Bar Association /Money Laundering and Terrorist Financing Prevention Act Information Service	2 employees
Dutch Gaming Authority	2 employees
Ministry of Finance	1 employee
Ministry of Security and Justice	1 employee
National Police	3 employees
Dutch Banking Association (NVB)	3 employees from 2 NVB member banks
Public Prosecution Service	2 employees
Tilburg University	1 employee
Leiden University, Institute for Security and Global Affairs	1 employee
Utrecht University	1 employee
VU University Amsterdam	1 employee

Appendix 3 List of participants in the expert meetings

In order to preserve the anonymity of the participants, this list gives only the names of the organisations where they are employed. In most cases, the same organisation representative took part in both expert meetings. Where this is not the case, a distinction is made between 'employee I' and 'employee II'.

Organisation	1st expert meeting	2nd expert meeting
Anti Money Laundering Centre	Employee I	Employee I
Netherlands Authority for the Financial Markets	Employee I	Employee I
Financial Supervision Office	Employee I	Employee I
Wwft Supervision Office	Employee I	Employee I
Dutch Central Bank	Employee I	Employee II
Customs Netherlands	Employee I	Employee I
FIU Netherlands	Employee I	Employee II
Holland Quaestor	Employee I	*Invited, no representative*
Dutch Gaming Authority	-*	Employee I
Royal Netherlands Marechaussee	Employee I	*Invited, no representative*
Royal Dutch Association of Civillaw Notaries	Employee I	Employee I
National Police	*Invited, no representative*	*Invited, no representative*
Netherlands Institute of Chartered Accountants	Employee I	Employee I
Netherlands Bar Association	Employee I	Employee I
Dutch Banking Association	Employee I	Employee I
Netherlands Association of Brokers and Appraisers	Employee I	Employee I
Netherlands Association of Financial Transaction Agencies	Employee I	Employee I
Public Prosecution Service	Employee I	Employee I

* After the first expert meeting it was discovered that the invitation had never reached the Dutch Gaming Authority employee.

Appendix 4 Expert meeting scripts

Script: first expert meeting

This document outlines the structure of the first expert meeting (completion of the impact matrix) held with money-laundering experts (on 9 May 2017).

Welcome and information on NRAs by the Research and Documentation Centre (WODC, 10 min.)

- WODC welcomes the attendees and asks them all to introduce themselves briefly.
- WODC provides some information on the NRAs and the research being conducted.
- WODC briefly explains the applicable methodology, concepts and definitions, and distributes the first handout containing this information.

Welcome and information on the expert meeting by APE Public Economics (10 min.)

- Welcome and introductions by APE.
- APE explains the expert meeting:
- This is the first meeting to be held as part of the analysis of money-laundering risks. Its purpose is to identify key money-laundering risks, and to estimate their potential impact. Today's session will run as follows:
  - We will look at a *longlist* of threats, compiled through an e-mail questionnaire, interviews with researchers and representatives of expert organisations, and analysis of six foreign NRAs, the European Supranational Risk Assessment (SNRA) and other relevant reports. The sector contributed to the creation of the longlist. What we ask is that you select the ten threats that you believe represent the greatest potential impact. To do so, we will use a Group Decision Room (GDR).
  - Once all of the participants have reached agreement on the ten threats representing the greatest potential impact, they will no longer be referred to as ‘threats’, but as ‘risks’.
  - Of these ten risks, we will then estimate the potential risk level presented by each, using a Multi Criteria Analysis (MCA) in the GDR.
  - The MCA will ask you to estimate the potential impact of each risk based on seven criteria. For example: we will ask you to estimate the size of the detrimental effect that ‘online gaming’ can exert on the ‘stability of the financial system’ on a scale of 0-100 (where 100 = maximum potential impact).
  - This means estimating the maximum potential impact/damage, i.e. in a hypothetical situation in which there is no anti-money-laundering policy. More on this later.
  - During the second expert meeting, policy experts will be asked to gauge the effectiveness of anti-money-laundering policy against the levels of risk assessed by you.
  - Your assessment today will produce a list of the ten main money-laundering risks, ranked according to potential risk impact.
  - This meeting will be run using a Group Decision Room (GDR). You will be asked several questions; your responses will be aggregated and projected on the screen in real time, and the results will then provide input for a discussion. The MCA will also take place in the GDR.
  - APE will explain that a meeting report will be drawn up, based on the attendees' digital responses and discussion. To avoid factual errors in the

reports, they will be sent to the experts who will have the opportunity to correct any inaccuracies. The final report will not present any results that can be traced back to individuals.

View the longlist of threats and add any additional threats (20 min.)

- The WODC distributes the handout with the thirty threats, and asks the experts to look at it. The WODC will also explain how the longlist was created, and experts can ask any questions at this point.
- APE asks the participants to add a maximum of two additional threats, if they believe any are missing. It will be emphasised that the threats on the longlist are at a certain level of abstraction; the experts are asked to consider this when adding threats to the list, which they can do via the GDR.

Look at the overview of money-laundering threats below. If you believe any key threats are missing, you may add up to two to the list. If you do not think there is anything missing, you can skip this question.

- The additional threats will be shown to the entire group.
- All of the threats will then be viewed and discussed in plenary. One key aim of this process is to merge any similar or overlapping threats, and to check whether the additional threats are genuinely missing from the longlist (or if they are already covered by any of the existing threats). Any additional threats remaining will be added to the longlist of money-laundering threats.

Selecting the main threats – two rounds (20 min.)

- The supplemented longlist will be presented digitally to the experts, who will be asked to select what they believe to be the ten key threats. The participants do so via the GDR.

From the list below, choose the ten threats you believe to be the most significant.

- The results will be projected to the group in a clear format, making it easy to see which threats the experts consider most significant. A frequency distribution of the longlisted threats (including additions) will be used.
- The experts will then be asked to explain their decision to the group. APE will guide the discussion towards the threats falling on either side of tenth place.
- After the explanations and discussion, the fifteen highest threats on the list will be presented digitally once more, and the experts will once again be asked to choose the ten threats they believe to be the most significant from the list. The reason for the second round is to allow for the possibility that the experts may have changed their minds after the discussion. The participants do so via the GDR.

From the list below, once again choose the ten threats you believe to be the most significant.

- The results will be presented to the group, and the top ten risks finalised. These threats – referred to from now on as ‘risks’ – will be further examined over the course of the meeting.

WODC explains the criteria (10 min.)

- The experts will now be asked to estimate the potential impact of the risks, based on the extent to which they can have a disruptive or detrimental effect on:
  a the stability of the financial system;

b the regular economy;
c society (civil and legal order);
d the degree to which regular society is interwoven with the criminal underworld;
e the manifestation or facilitation of crime or terrorist activities;
f the (perceived) feeling of public safety;
g the image/reputation of the Netherlands.

- The WODC will present these criteria to the experts and explain them in greater detail, and distribute a handout including the numbered criteria (a-g). Next, it will be proposed to adopt the list of criteria. In principle, the criteria cannot be changed: the relevance and completeness of the list are not open to discussion.
- The experts are once again instructed to estimate the severity of the selected risks using the seven criteria, and are asked to gauge the extent to which each risk can have a disruptive or detrimental effect on each of the criteria.

Weighting (15 min.)

- The experts are to assign a weighting to each of the criteria, expressing its importance in both an absolute sense and relative to the other criteria. This step is included, as we do not expect the experts to consider all of the criteria to be of equal importance. Each criterion receives a weighting from 1-10 (where 10 = most important). The experts perform the weighting digitally and individually:

Weight each criterion from 1-10 (where 10 = most important). The weighting expresses the importance of each criterion in both an absolute sense and relative to the other criteria.

- The average weightings will be calculated immediately, then displayed on-screen and discussed by the group. The standard deviation for each of the criteria will also be made available for discussion.
- A digital poll will then be held on the average weighting of each criterion. The participants will be shown the seven criteria, along with the associated average weightings. This is important, as the experts need to be able to judge the weightings relative to one another.

Look at the average weighting of each criterion. Do you agree?

- If the majority of the experts agree with the average weighting, it will be officially adopted.
- If, after the first poll, over half of the experts do not agree with the average weighting, those for and against will be asked to state their reasons, after which the experts can vote once again. The average will be finalised after the second poll.

Break (15 min.)

After the break, the MCA will be carried out: the potential impact of the selected risks will be determined by the weighted averages of the experts' opinions.

The impact matrix (25 min.)

- Experts gauge the extent to which each of the risks can produce a detrimental or other impact. They do so individually, using the digital environment.
- When making their judgements, the experts must consider the Dutch context (e.g. geographic location) and therefore also the likelihood that a risk will have a detrimental effect, to the extent that the likelihood is determined by the context.

- The experts must *not* consider any existing policy that may help to limit the extent of any negative/other consequences. This means estimating the maximum potential damage, i.e. in a hypothetical situation in which there is no anti-money-laundering policy.
- The experts estimate the potential impact of the risks, based on the extent to which they can (or do) have a disruptive or detrimental effect on the seven criteria.
- Each expert is asked to complete the matrix vertically, to ensure that the evaluation of each criterion is made in the same way for each risk.
- WODC briefly explains how the experts can rate the extent to which a risk may have a disruptive or detrimental effect on each of the criteria, or in other words, how the scale from 0-100 can be interpreted. To this end, a handout will be issued dividing the 0-100 scale into categories.

Complete the matrix below, rating the extent to which the risk may have a detrimental or disruptive effect on each of the criteria. Score each risk-criterion pair from 0-100, where 0 = no impact and 100 = maximum impact.

- A total aggregated score will be calculated for each risk by taking the weighted average of the extent to which each risk can have a disruptive or detrimental effect on each of the seven criteria.
- These weighted averages will be displayed to the group, allowing the risks to be ranked in order for the first time.

Discussion of matrix results (35 min.)
- The rankings will be displayed to the entire group, and the experts asked to substantiate their scores based on the rankings and the degree of consensus (expressed by the standard deviation of the ten total scores on the underlying criteria). This will clarify which considerations, information and concrete experiences experts used to arrive at their judgements. Probing questions are important at this stage, as well as asking for supporting sources of data and concrete experiences. If these sources are absent or insufficient, the experts will be asked what data they feel they need in order to arrive at an informed opinion. Sufficient time will be devoted to this process.

Opportunity to modify the matrix (5 min.)
- The experts are now given the opportunity to modify their individual impact matrices, adjusting their risk assessments based on the preceding discussion and comments by other experts.

Discussing the risk rankings and finalising the order (15 min.)
- The average total scores (following any modifications) will be displayed to and discussed by the group.
- The experts will be asked to make any additional comments on the ranking.
- The outcome of this exercise will be a ranked list of the ten greatest money-laundering-related risks according to expert opinions and judgements.

Conclusion (5 min.)
- APE and the WODC thank all participants for their time and input.

Second meeting

This document outlines the structure of the second expert meeting (determining resilience scores) held with money-laundering experts (on 30 May 2017).

Welcome and information on NRAs by the Research and Documentation Centre (WODC, 10 min.)

- WODC welcomes the attendees and asks them all to introduce themselves briefly.
- WODC provides brief information on the NRAs and current/future research.
- WODC briefly explains the definition of *resilience* and distributes the first handout containing this information. Resilience relates to the available organisational, municipal, national and international policy instruments, as well as their implementation (the extent to which the instruments are put to use).

Welcome and information on the expert meeting by APE Public Economics (5 min.)

- Welcome and introductions by APE.
- APE explains the expert meeting:
- This is the second meeting to be held as part of the analysis of money-laundering risks, and will concentrate on the resilience of policy instruments. The aim of this second meeting is to establish how effectively the currently available policy instruments combat money-laundering risks. The meeting will be run as follows:
  - You will be asked to estimate the effectiveness of existing policy with relation to a total of ten risks (those risks identified during the previous meeting, for which an initial risk analysis has been produced). The potential impact of these risks has already been determined, however without any consideration of the resilience of existing policy in combating that impact. That will be your task for today, in order to increase the value of the risk analysis.
  - Later in the process we will ask you to identify the policy instruments that combat the ten risks, and gauge the resilience of each instrument.
  - You will then be asked to estimate the resilience of existing policy a second time, and discuss the results. This assessment will be used to determine the level of risk remaining (the residual risk) once the relevant policy has been taken into consideration. The ultimate result will be a list of ten risks, ranked according to risk level.
- This meeting will be run using a group discussion room (GDR). You will be asked several questions; your responses will be aggregated and projected on the screen in real time, and the results will then provide input for a discussion.
- APE will explain that a meeting report will be drawn up, based on the attendees' digital responses and discussion. To avoid factual errors in the reports, they will be sent to the experts who will have the opportunity to correct any inaccuracies. The final report will not present any results that can be traced back to individuals.

Information on the identified risks (WODC, 5 min.)

- The WODC will distribute the handout containing the ten risks that were identified and analysed in the previous meeting.
- The risks and the ranking will be discussed, and the experts informed that anti-money-laundering policy was not considered when estimating the risk level.

First resilience assessment (5 min.)

- APE asks the experts to make an initial assessment of the resilience of existing policy. The participants are asked to enter a resilience score for each risk, using the GDR:

Please indicate the percentage to which you believe each of the risks is combated by the available policy instruments. You may also state that you do not believe you have enough knowledge or experience to give an informed opinion.

- The results will not be discussed straight away; we will ask the participants to make a second assessment later, after which the results will be discussed. Any differences in the average resilience scores will also be discussed at that time.

Determining the effect of each instrument (110 min.)

- WODC will distribute a handout listing four policy instruments (Acts), and give an explanation. These four instruments are all relevant to combating money-laundering risks.
- APE will ask the experts to indicate the extent to which each of the various instruments contributes to the resilience of the range of instruments as a whole.
- The first step will involve identifying the policy instruments relevant to each risk, by asking the group as a whole which instruments these are (in addition to the four major Acts).
- In step 2, the experts will be asked to evaluate the contribution made by each of the (original and additional) instruments to the resilience of the available policy instruments as a whole. They do so using the GDR. The experts will only be asked to give an estimation for a risk if they have provided a resilience score for that risk. Those who did not will be asked to skip the risk in question.

Please indicate the extent to which each of the policy instruments below contributes to combating the given risk. You have 100 points to distribute across the policy instruments, where more points reflects a greater contribution.

- The average results for each instrument will be shown to the group. The experts will be asked to substantiate their answers, based on the averages displayed and the level of consensus (expressed as a standard deviation).

Second resilience assessment (5 min.)

- APE will ask the participants to revise their previous assessment (if their opinion has changed), by altering their initial responses directly in the GDR.

Discussion of the final resilience assessment (20 min.)

- The average resilience scores for each risk will be displayed to the group. The experts will be asked to substantiate their answers, based on the averages displayed and the level of consensus (expressed as a standard deviation).
- They will also be asked to name any *problem areas* affecting the resilience of policy instruments (these will mostly relate to poor information exchange).
- *Improvement potential* will be a second focus area during this discussion. Experts will be asked to name any opportunities they see for improving the resilience of anti-money-laundering policy, and to estimate the time necessary to realise the benefits.

Calculation and discussion of residual risk (15 min.)

- The resilience scores will be used to calculate the risk scores.
- The risks will be displayed in order of residual risk.
- The experts will be asked to make any additional comments on the ranking.

Conclusion (5 min.)

- WODC will remind the experts of the outstanding e-mail consultation on data sources, and ask them to complete it.
- APE and the WODC thank all participants for their time and input.

Appendix 5 Results of the first expert meeting

Threats

In the Group Decision Room experts were asked to look at the overview of money-laundering threats below. If they believed any key threats were missing, they could add up to two threats to the list.

Threats
Purchase/overhaul of real estate using illegal or untraceable funds
Online gambling
Straw men
Spending below the disclosure threshold with organisations under a disclosure obligation
Money laundering using prepaid cards, debit cards, telephone cards, etc.
Use of virtual currencies (e.g. bitcoin, crypto-currencies)
Complex corporate structures via trust offices
Constructions for concealing actual value, such as loan-backs and/or usage constructions (e.g. lease) instead of legal property (e.g. in the real-estate sector)
Non-transparent cash flows from abroad (PEPs)
ABC-constructions (e.g. real estate)
Use of offshore companies/international transactions to/from offshore territories
Money laundering via fiscally driven/complex corporate structures
Using national and international investment structures for value transfer
Turnover/price manipulation
Over/underbilling within national/international commerce
National and international trade offering opportunities for criminals to transfer value or to legitimise growth or loss in value and obscuring whether transactions are associated with a goods flow, what the origin of the goods flow is, and/or whether a goods flow even exists
Exchanging small cash denominations for larger ones (and vice versa)
Introducing cash funds into the electronic payments system
Converting cash funds into valuable goods (precious metals, art, jewellery etc.)
Physical transport of cash into/out of the Netherlands
Transferring cash funds via underground/unlicensed banks (e.g. Hawala)
Large cash deposits
Money laundering via unregulated payment service providers (PSP)
Money laundering via money transfer companies
Money laundering via accountants
Money laundering via financial institutions
Money laundering via trust offices
Use of third parties' accounts via lawyers
Use of third parties' accounts' via civillaw notaries
Addition: Bankruptcy fraud
Addition: Money laundering via foundations
Addition: Identity fraud
Addition: VAT abuse
Modification: Expenditure at and transfer of assets to non-obliged entities

Round 1: From the list below, choose the ten threats you believe to be the most significant

Threats	Times selected
Use of offshore companies/international transactions to/from offshore territories	12
National and international commercial transactions offering opportunities for criminals to transfer value or to legitimise growth or loss in value and obscuring whether transactions are associated with a goods flow, what the origin of the goods flow is, and/or whether a goods flow even exists	11
Money laundering via fiscally driven/complex corporate structures	10
Money laundering via trust offices	9
Constructions for concealing actual value, such as loan-backs and/or usage constructions (e.g. lease) instead of legal property (e.g. in the real-estate sector)	8
Physical transport of cash into/out of the Netherlands	7
Straw men	7
Non-transparent cash flows from abroad (PEPs)	7
Money laundering via payment service providers	7
Transferring cash funds via underground/unlicensed banking (e.g. Hawala)	7
Complex corporate structures via trust offices	6
ABC-constructions (e.g. real estate)	6
Money laundering via financial institutions	6
Use of virtual currencies	5
Using national and international investment structures for value transfer	5
Money laundering via foundations	5
Introducing cash funds into the electronic payments system	5
Converting cash funds into valuable goods (precious metals, art, jewellery etc.)	5
Large cash deposits	5
Money laundering via unregulated payment service providers (PSP)	4
Over/underbilling within national/international commerce	4
Turnover and/or price manipulation	4
Identity fraud	3
VAT abuse	2
Use of 'derdengeldenrekeningen' via lawyers	2
Expenditure at and transfer of assets to non-obliged entities	2
Purchase/overhaul of real estate using illegal or untraceable funds	1
Bankruptcy fraud	1
Exchanging small cash denominations for larger ones (and vice versa)	1
Use of 'derdengeldenrekeningen' via civil law notaries	1
Money laundering using prepaid cards, debit cards, telephone cards, etc.	1
Expenditure below the monetary threshold with obliged entities	1
Money laundering via accountants	0
Online gambling	0

Round 2: From the list below, once again choose the ten threats you believe to be the most significant

Threats	Times selected
Use of offshore companies/international transactions to/from offshore territories	15
National and international commercial transactions offering opportunities for criminals to transfer value or to legitimise growth or loss in value and obscuring whether transactions are associated with a goods flow, what the origin of the goods flow is, and/or whether a goods flow even exists	15
Money laundering via trust offices	14
Money laundering via fiscally driven/complex corporate structures	13
Money laundering via payment service providers	13
Use of virtual currencies	13
Money laundering via financial institutions	12
Merged threats: Transferring cash funds via underground/unlicensed banking (e.g. Hawala) + physical transport of cash into/out of the Netherlands	11
Constructions for concealing actual value, such as loan-backs and/or usage constructions (e.g. lease) instead of legal property (e.g. in the real-estate sector)	10
Using national/international investment structures for value transfer	10
Straw men	10
Non-transparent cash flows from abroad (PEPs)	7
Complex corporate structures through trust offices	7
ABC-constructions (e.g. real estate)	7

Criteria

Weight each criterion from 1-10 (where 10 = most important). The weighting expresses the importance of each criterion in both an absolute sense and relative to the other criteria.

Criteria	Average score	Standard deviation
D The degree to which regular society is interwoven with the criminal underworld	8.3	1.2
E The manifestation or facilitation of crime or terrorist activities	7.8	1.8
A The stability of the financial system	7.6	1.8
C Society (civil and legal order)	6.9	2.4
B The regular economy	6.7	1.5
G The image/reputation of the Netherlands	6.3	2.9
F The (perceived) feeling of public safety	4.4	2.4

Matrix

Complete the matrix below, judging the extent to which each threat may have a detrimental or disruptive effect on each of the criteria. Score each risk-criterion pair from 0-100, where 0 = no potential impact and 100 = maximum potential impact.

A The stability of the financial system – Weighting: 8
B The regular economy – Weighting: 7
C Society (civil and legal order) – Weighting: 7
D The degree to which regular society is interwoven with the criminal underworld – Weighting: 8
E The manifestation or facilitation of crime or terrorist activities – Weighting: 8

F The (perceived) feeling of public safety – Weighting: 4
G The image/reputation of the Netherlands – Weighting: 6

Risk	A	B	C	D	E	F	G	Average
Money laundering via financial institutions (especially banks)	96.2	68.1	69.6	95.9	89.2	27.9	62.7	72.8
Money laundering via payment service providers	86.8	60.4	56.9	89.5	89.4	25.2	61.4	67.1
Money laundering via trust offices	76.6	57.9	47.9	98.6	85.9	18.3	69.1	64.9
Money laundering via offshore firms	71.0	63.0	45.3	90.0	86.4	16.1	61.4	61.9
Trade-Based Money Laundering	61.1	67.7	42.9	88.7	88.3	15.6	48.1	58.9
Money laundering constructions to conceal actual value	64.9	52.4	48.0	87.7	82.1	19.8	57.6	58.9
Money laundering via fiscally driven/complex corporate structures	63.5	54.2	44.7	84.7	79.5	15.7	62.2	57.8
Money laundering via virtual currencies	73.6	48.4	50.0	60.0	90.5	25.5	47.3	56.4
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	60.2	52.3	53.1	64.8	88.2	25.6	44.5	55.5
Money laundering via national and international investment structures for value transfer	67.6	51.4	39.0	82.4	73.0	16.0	57.9	55.3

Money laundering via financial institutions (especially banks)

Criteria	Average score	Standard deviation
A The stability of the financial system	82.5	14.1
B The regular economy	66.7	21.8
C Society (civil and legal order)	68.1	21.1
D The degree to which regular society is interwoven with the criminal underworld	82.2	9.6
E The manifestation or facilitation of crime or terrorist activities	76.5	19.2
F The (perceived) feeling of public safety	47.9	25.2
G The image/reputation of the Netherlands	71.6	15.2

Money laundering via payment service providers

Criteria	Average score	Standard deviation
A The stability of the financial system	74.4	20.0
B The regular economy	59.2	22.3
C Society (civil and legal order)	55.7	28.8
D The degree to which regular society is interwoven with the criminal underworld	76.7	15.7
E The manifestation or facilitation of crime or terrorist activities	76.7	14.6
F The (perceived) feeling of public safety	43.1	21.6
G The image/reputation of the Netherlands	70.2	14.1

Money laundering via trust offices

Criteria	Average score	Standard deviation
A The stability of the financial system	65.7	20.9
B The regular economy	56.7	22.1
C Society (civil and legal order)	46.9	25.4
D The degree to which regular society is interwoven with the criminal underworld	84.5	11.8
E The manifestation or facilitation of crime or terrorist activities	73.6	16.8
F The (perceived) feeling of public safety	31.4	20.6
G The image/reputation of the Netherlands	79.0	12.7

Money laundering via offshore firms

Criteria	Average score	Standard deviation
A The stability of the financial system	60.9	25.1
B The regular economy	61.7	21.1
C Society (civil and legal order)	44.4	26.2
D The degree to which regular society is interwoven with the criminal underworld	77.1	12.5
E The manifestation or facilitation of crime or terrorist activities	74.1	16.7
F The (perceived) feeling of public safety	27.7	18.3
G The image/reputation of the Netherlands	70.1	18.8

Trade-Based Money Laundering

Criteria	Average score	Standard deviation
A The stability of the financial system	52.4	25.3
B The regular economy	66.3	20.5
C Society (civil and legal order)	42.0	26.3
D The degree to which regular society is interwoven with the criminal underworld	76.0	15.0
E The manifestation or facilitation of crime or terrorist activities	75.7	18.9
F The (perceived) feeling of public safety	26.7	21.1
G The image/reputation of the Netherlands	55.0	26.8

Money laundering constructions to conceal actual value

Criteria	Average score	Standard deviation
A The stability of the financial system	55.7	16.6
B The regular economy	51.3	23.6
C Society (civil and legal order)	47.0	23.2
D The degree to which regular society is interwoven with the criminal underworld	75.2	14.2
E The manifestation or facilitation of crime or terrorist activities	70.4	18.6
F The (perceived) feeling of public safety	33.9	18.4
G The image/reputation of the Netherlands	65.8	11.2

Money laundering via fiscally driven / complex corporate structures

Criteria	Average score	Standard deviation
A The stability of the financial system	54.5	21.8
B The regular economy	53.1	21.2
C Society (civil and legal order)	43.8	21.2
D The degree to which regular society is interwoven with the criminal underworld	72.6	17.7
E The manifestation or facilitation of crime or terrorist activities	68.1	17.2
F The (perceived) feeling of public safety	26.9	16.1
G The image/reputation of the Netherlands	71.1	18.8

Money laundering via virtual currencies

Criteria	Average score	Standard deviation
A The stability of the financial system	63.1	24.8
B The regular economy	47.4	20.9
C Society (civil and legal order)	48.9	22.0
D The degree to which regular society is interwoven with the criminal underworld	51.4	27.1
E The manifestation or facilitation of crime or terrorist activities	77.5	17.6
F The (perceived) feeling of public safety	43.7	18.8
G The image/reputation of the Netherlands	54.0	27.7

Money laundering via relocation of cash funds to / from the Netherlands (via underground banking or otherwise)

Criteria	Average score	Standard deviation
A The stability of the financial system	51.6	28.9
B The regular economy	51.3	25.1
C Society (civil and legal order)	52.0	23.2
D The degree to which regular society is interwoven with the criminal underworld	55.5	24.8
E The manifestation or facilitation of crime or terrorist activities	75.6	21.1
F The (perceived) feeling of public safety	43.9	28.3
G The image/reputation of the Netherlands	50.8	21.9

Money laundering via national and international investment structures for value transfer

Criteria	Average score	Standard deviation
A The stability of the financial system	57.9	20.7
B The regular economy	50.3	23.8
C Society (civil and legal order)	38.2	22.5
D The degree to which regular society is interwoven with the criminal underworld	70.7	16.0
E The manifestation or facilitation of crime or terrorist activities	62.6	18.0
F The (perceived) feeling of public safety	27.5	18.8
G The image/reputation of the Netherlands	66.2	16.4

New matrix following the discussion

Risk	A	B	C	D	E	F	G	Average
Money laundering via financial institutions (especially banks)	96.2	68.1	70.2	95.9	89.2	27.9	62.7	72.9
Money laundering via payment service providers	82.5	58.4	54.9	87.2	87.1	25.2	59.7	65.0
Money laundering via trust offices	76.6	57.9	47.9	98.6	85.9	18.3	69.1	64.9
Money laundering via offshore firms	71.0	63.0	45.3	90.0	86.4	16.1	61.4	61.9
Money laundering constructions to conceal actual value	64.9	52.4	48.0	87.7	82.1	19.4	57.6	58.9
Trade-Based Money Laundering	61.1	67.7	42.9	88.7	88.3	14.8	48.1	58.8
Money laundering via fiscally driven/complex corporate structures	63.5	54.2	46.1	84.7	79.5	15.7	62.2	58.0
Money laundering via virtual currencies	75.1	49.1	52.0	65.4	93.6	25.5	44.9	57.9
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	57.9	51.7	52.4	64.0	90.9	28.6	45.0	55.8
Money laundering via national and international investment structures for value transfer	67.6	49.3	37.0	84.8	70.7	15.2	57.8	54.6

Impact assessment of the ten risks (on a scale from 0-100)

Risk	1st assessment of potential impact	2nd assessment of potential impact	Compared to 1st assessment
Money laundering via financial institutions (especially banks)	73	73	-
Money laundering via payment service providers	67	65	-2 points
Money laundering via trust offices	65	65	-
Money laundering via offshore firms	62	62	-
Money laundering constructions to conceal actual value	59	59	-
Trade-Based Money Laundering	59	59	-
Money laundering via fiscally driven/complex corporate structures	58	58	-
Money laundering via virtual currencies	56	58	+2 points
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	56	56	-
Money laundering via national and international investment structures for value transfer	55	55	-

Appendix 6 Results of the second expert meeting

First resilience assessment

Please indicate the percentage to which you believe each of the risks is combated by the available policy instruments.

Risk	Average score (0-100%)	Standard deviation
Money laundering via financial institutions (especially banks)	49.1	17.7
Money laundering via payment service providers	45.0	20.8
Money laundering via trust offices	41.9	20.2
Money laundering via offshore firms	26.5	19.8
Money laundering constructions to conceal actual value	29.5	23.5
Trade-Based Money Laundering	27.3	17.3
Money laundering via fiscally driven/complex corporate structures.	37.7	20.0
Money laundering via virtual currencies	13.6	14.2
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	29.6	20.3
Money laundering via national and international investment structures for value transfer	32.1	16.4
Average	33.2	21.4

Policy instruments

Please indicate the extent to which each of the policy instruments below contributes to combating the given risk. You have 100 points to distribute across the policy instruments, where more points reflects a greater contribution.

Money laundering via financial institutions (especially banks)

Policy instruments	Average score	Standard deviation
The Money Laundering and Terrorist Financing Prevention Act	33.2	13.8
The Financial Supervision Act	19.7	9.2
Dutch Penal Code	10.5	8.4
General terms and conditions of banks	7.8	7.8
The Trust and Company Service Providers (Supervision) Act	6.5	5.6
Wet Bibob	6.4	6.7
Incident referral protocol (ERA register)	5.3	5.8
Nationally-applicable EU legislation (information on wire transfers)	4.8	4.2
Commercial Register Act (incl. UBOs)	4.2	3.8
Audit Firms (Supervision) Act	1.7	2.2

Money laundering via payment service providers

Policy instruments	Average score	Standard deviation
The Money Laundering and Terrorist Financing Prevention Act	37.7	11.8
The Financial Supervision Act	26.8	6.8
Dutch Penal Code	13.2	6.6
Nationally-applicable EU legislation (information on wire transfers)	7.5	8.5
Commercial Register Act (incl. UBOs)	4.0	5.9
Wet Bibob	3.2	5.7
General terms and conditions of banks	3.1	5.8
Incident referral protocol (ERA register)	2.2	2.8
The Trust and Company Service Providers (Supervision) Act	1.2	4.0
Audit Firms (Supervision) Act	1.0	2.7

Money laundering via trust offices

Policy instruments	Average score	Standard deviation
The Trust and Company Service Providers (Supervision) Act	31.7	11.5
The Money Laundering and Terrorist Financing Prevention Act	28.2	8.1
Tax legislation	14.3	4.5
Dutch Penal Code	9.1	6.5
Commercial Register Act (incl. UBOs)	7.8	7.6
Wet Bibob	2.4	6.7
Nationally-applicable EU legislation (information on wire transfers)	2.2	4.3
General terms and conditions of banks	1.7	3.0
The Financial Supervision Act	1.5	4.1
Audit Firms (Supervision) Act	1.2	2.3
Incident referral protocol (ERA register)	0.0	0.0

Money laundering via offshore firms

Policy instruments	Average score	Standard deviation
The Money Laundering and Terrorist Financing Prevention Act	29.9	10.9
Tax legislation	15.4	7.8
International treaties	14.6	6.1
The Trust and Company Service Providers (Supervision) Act	11.1	13.4
Dutch Penal Code	10.5	5.5
Commercial Register Act (incl. UBOs)	5.7	6.6
Nationally-applicable EU legislation (information on wire transfers)	4.3	6.2
The Financial Supervision Act	3.8	6.5
Audit Firms (Supervision) Act	1.8	3.9
General terms and conditions of banks	1.4	2.8
Wet Bibob	1.4	5.2
Incident referral protocol (ERA register)	0.0	0.0

Money laundering constructions to conceal actual value

Policy instruments	Average score	Standard deviation
The Money Laundering and Terrorist Financing Prevention Act	30.4	11.6
Tax legislation	20.5	16.0
Dutch Penal Code	17.4	9.5
The Financial Supervision Act	6.6	9.6
Audit Firms (Supervision) Act	5.7	8.0
Wet Bibob	5.6	7.5
Commercial Register Act (incl. UBOs)	4.8	7.0
Nationally-applicable EU legislation (information on wire transfers)	4.5	6.0
The Trust and Company Service Providers (Supervision) Act	3.3	5.3
General terms and conditions of banks	1.1	2.8
Incident referral protocol (ERA register)	0.0	0.0

Trade-Based Money Laundering

Policy instruments	Average score	Standard deviation
Nationally-applicable EU legislation (information on wire transfers), esp. customs legislation	30.1	12.2
Tax legislation	23.1	7.3
The Money Laundering and Terrorist Financing Prevention Act	22.2	11.0
Dutch Penal Code	10.8	6.4
Commercial Register Act (incl. UBOs)	4.9	5.4
Audit Firms (Supervision) Act	2.7	4.0
Wet Bibob	2.6	4.4
The Financial Supervision Act	1.9	3.7
The Trust and Company Service Providers (Supervision) Act	1.4	3.2
General terms and conditions of banks	0.1	0.5
Incident referral protocol (ERA register)	0.0	0.0

Money laundering via fiscally driven/complex corporate structures

Policy instruments	Average score	Standard deviation
Tax legislation	28.8	8.1
The Money Laundering and Terrorist Financing Prevention Act	27.9	8.0
The Trust and Company Service Providers (Supervision) Act	11.6	9.6
Commercial Register Act (incl. UBOs)	10.1	6.1
Audit Firms (Supervision) Act	6.2	6.8
Dutch Penal Code	6.1	6.7
The Financial Supervision Act	4.0	5.4
Wet Bibob	2.6	5.6
Nationally-applicable EU legislation (information on wire transfers)	1.9	3.2
General terms and conditions of banks	0.5	1.3
Incident referral protocol (ERA register)	0.2	0.8

Money laundering via virtual currencies

Policy instruments	Average score	Standard deviation
The Money Laundering and Terrorist Financing Prevention Act	38.5	9.2
Dutch Penal Code	20.1	9.5
The Financial Supervision Act	16.8	12.0
General terms and conditions of banks	11.5	13.4
Nationally-applicable EU legislation (information on wire transfers)	5.4	7.9
Audit Firms (Supervision) Act	2.5	3.8
The Trust and Company Service Providers (Supervision) Act	1.8	3.9
Incident referral protocol (ERA register)	1.6	2.8
Commercial Register Act (incl. UBOs)	1.3	2.8
Wet Bibob	0.5	1.4

Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)

Policy instruments	Average score	Standard deviation
The Money Laundering and Terrorist Financing Prevention Act	25.3	14.7
Dutch Penal Code	23.9	13.4
Nationally-applicable EU legislation (information on wire transfers)	20.5	15.1
The Financial Supervision Act	14.9	13.2
Tax legislation	9.5	9.4
General terms and conditions of banks	2.8	4.3
Wet Bibob	0.9	2.0
Incident referral protocol (ERA register)	0.9	2.8
The Trust and Company Service Providers (Supervision) Act	0.8	2.5
Commercial Register Act (incl. UBOs)	0.3	1.2
Audit Firms (Supervision) Act	0.3	0.7

Money laundering via national and international investment structures for value transfer

Policy instruments	Average score	Standard deviation
The Money Laundering and Terrorist Financing Prevention Act	23.2	9.3
Tax legislation	22.0	7.1
The Financial Supervision Act	17.1	9.9
Dutch Penal Code	13.6	8.2
Wet Bibob	7.7	15.0
The Trust and Company Service Providers (Supervision) Act	4.1	6.1
Audit Firms (Supervision) Act	3.8	5.0
Nationally-applicable EU legislation (information on wire transfers)	3.6	6.3
Commercial Register Act (incl. UBOs)	2.6	2.9
General terms and conditions of banks	1.3	2.5
Incident referral protocol (ERA register)	1.1	2.5

Second resilience assessment

Please indicate the percentage to which you believe each of the risks is combated by the available policy instruments.

Risk	Average score (0-100%)	Standard deviation
Money laundering via financial institutions (especially banks)	48.6	18.0
Money laundering via payment service providers	40.5	15.7
Money laundering via trust offices	39.2	17.2
Money laundering via fiscally driven/complex corporate structures	36.9	19.7
Money laundering via national and international investment structures for value transfer	30.8	17.2
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	28.2	18.9
Trade-Based Money Laundering	27.3	17.1
Money laundering constructions to conceal actual value	26.8	15.6
Money laundering via offshore firms	26.5	18.2
Money laundering via virtual currencies	13.2	12.8
Average	31.7	19.5

Comparison between the first and second resilience assessment

Average estimated resilience of the entire range of policy instruments for each risk (from 0-100%)

	1st assessment resilience	2nd assessment resilience	Compared to 1st assessment
Money laundering via financial institutions (especially banks)	49%	49%	-
Money laundering via payment service providers	45%	41%	-4 percentage points
Money laundering via trust offices	42%	39%	-3 percentage points
Money laundering via fiscally driven/complex corporate structures	38%	37%	-1 percentage point
Money laundering via national and international investment structures for value transfer	32%	31%	-1 percentage point
Money laundering via relocation of cash funds to/from the Netherlands (via underground banking or otherwise)	30%	28%	-2 percentage points
Money laundering constructions to conceal actual value	30%	27%	-3 percentage points
Money laundering via offshore firms	27%	27%	-
Trade-Based Money Laundering	27%	27%	-
Money laundering via virtual currencies	14%	13%	-1 percentage point
Average resilience	33%	32%	-1 percentage point