FATF

Anti-money laundering and counter-terrorist financing measures

The Netherlands

Mutual Evaluation Report

August 2022

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org.**

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

This assessment was adopted by the FATF at its June 2022 Plenary meeting.

Citing reference:

FATF (2022), *Anti-money laundering and counter-terrorist financing measures – The Netherlands,* Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-netherlands-2022.html

Table of Contents

Executive Summary

1. This report summarises the anti-money laundering and counter-terrorist financing (AML/CFT) measures in place in the Kingdom of the Netherlands (hereafter referred to as the Netherlands) as at the date of the on-site visit (27 October – 18 November 2021). The report includes an assessment of Bonaire, St. Eustatius and Saba (hereafter referred to as the BES Islands) as these Caribbean islands form part of the Netherlands. This report analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

1. Overall, the Netherlands has a good understanding of its money laundering and terrorist financing (ML/TF) risks, as reflected in the National Risk Assessments (NRAs), Supranational Risk Assessments (SNRAs) and other sector assessments, policies, projects and cases. In continental Netherlands, fraud and drug related offences account for more than 90% of all proceeds of crime and ML risk manifests via the use of crypto currencies; trade-based services; underground banking, including unlicensed payment services; offshore companies; and services/goods of dealers of high-value goods. The methodology of the NRAs is generally sound and based on a structural process to collect and evaluate qualitative inputs from policy, supervisory, law enforcement and private sector authorities through extensive surveys, meetings and interviews. However, inputs into the NRAs can be strengthened by the inclusion of additional quantitative sources. A key strength of the Dutch system lies on its robust domestic co-ordination and co-operation on AML/CFT issues at both the policy and operational levels and it is a leader in public-private partnership and information sharing to combat ML/TF.

2. Competent authorities use a wide range of financial intelligence sources in their investigations, including data hubs, Financial Intelligence Unit (FIU) disseminations, inter-agency co-operation platforms and public-private partnerships. Law enforcement authorities (LEAs) increasingly access FIU disseminations and request information exchange on criminal and unexplained

wealth (iCOV) reports during their investigations into ML, TF and predicate offences. FIU products are of high quality, timely and targeted to law enforcement needs. Minor concerns exist on the lack of a feedback mechanism to the FIU on the follow-up given by LEAs to its disseminations and on the number of disseminations left unattended in the Police database; however, these issues are largely mitigated by the close operational co-operation between LEAs and FIU-NL.

3. LEAs initiated a significant number of ML investigations at both national and regional levels, and pursue different types of ML. The AML Strategic Programme and thematic investigation projects are two strengths of the Dutch system. Case studies on regional and national investigations are consistent with the ML channels and methods identified in the NRAs. The lack of statistics on predicate offences and on the type of ML pursued limits a comprehensive view of ML cases. The sanctions imposed in ML cases are low, including in complex and serious cases, and are therefore not considered dissuasive by the Assessment Team.

4. In the BES Islands, the expertise of LEAs to conduct financial investigations has improved, and a specialised ML Prosecutor role has been created. Nevertheless, LEAs are still reliant on the support from continental Netherlands for ML cases, especially for complex investigations. Authorities focus mainly on the prosecution of predicate offences, and the overall number of ML investigations and convictions is low.

5. The Netherlands pursues confiscation as a policy and strategic objective, supported by a solid legal and institutional framework and financial expertise. Competent authorities regularly seek object and value confiscation. The statistics available, even if not comprehensive, demonstrate that confiscation results are in line with national policies and the main proceeds-generating crimes. Confiscations in out of court settlements with legal persons account for the high majority of collected confiscation results. Netherlands has seized cash at the borders and initiated ML investigations, but some concerns remain in terms of the dissuasiveness of sanctions related to the cash declaration system.

6. The Netherlands has successfully detected, investigated and prosecuted TF generally in line with its risk profile, with a majority of cases involving the funding of foreign terrorist fighters (FTFs). While there have been some investigations of non-profit organisations (NPOs) possibly involved in TF, no conviction has been achieved, which is not in line with their high risk categorisation for TF in the NRA. Competent authorities co-operate closely on TF and terrorism investigations and regularly discuss any possible TF signal. Furthermore, partnerships with the private sector enable LEAs to gather additional insights into potential suspects. However, the level of sanctions imposed is generally low, which affects dissuasiveness. The authorities used various alternative measures when it was not practicable to obtain a TF conviction.

7. The Netherlands implements proliferation financing (PF) and TF targeted financial sanctions (TFS) without delay. As there is no supervision of the implementation of TFS without delay for DNFBPs other than trust offices, the authorities cannot determine to which extent these entities implement TFS obligations. Supervisors are not mandated to supervise the implementation of TFS obligations by these obliged entities and cannot impose sanctions or remedial actions. Similar deficiencies exist in the BES Islands for DNFBPs and VASPs. The understanding of TFS obligations is strong amongst financial institutions (FIs). TF

domestic designations have targeted mostly FTFs, resulting in small amounts frozen consistent with the risk profile.

8. Self-regulation is a key feature of the Dutch NPO sector. The Netherlands has proactively and extensively engaged NPOs to raise awareness on TF risks. The Netherlands has a robust understanding of the subset of NPOs most vulnerable to TF risk. This understanding could be improved by a specific sectoral risk assessment. Good faith NPOs which, by virtue of their activities, are more exposed to TF threats are well aware of the risks and already implement mitigating measures. However, the limited visibility on NPOs' financial activities is an obstacle in detecting and investigating NPOs that willingly sponsor terrorism.

9. Understanding of ML risk for FIs and virtual asset service providers (VASPs) is generally good, and policies and procedures are in place commensurate to risks. The same applies to trust offices, which are supervised by the Dutch Central Bank (DNB). For other designated non-financial businesses and professions (DNFBPs), understanding of ML risk and obligations varies and is generally more limited. The understanding of TF risk is lower across all obliged entities.

10. Where a legal person has no beneficial owner (BO) (e.g., in the case of some foundations and associations) or in exceptional circumstances where it is not possible to identify the ultimate BO, Dutch legislation allows the registration of senior managing directors as 'pseudo' BOs[1]. Some FIs and most DNFBPs struggle to identify the ultimate BOs of legal persons that are part of complex structures or have international components. In such circumstances, the obliged entities can fall back too quickly on the legally permitted option to register the 'pseudo-BOs'.

11. In some cases, FIs—including larger banks—tend to classify too many customers as low risk without adequate justification. Obliged entities in most sectors generally understand and implement their reporting obligations, but unusual transaction reports (UTRs) filed in some sectors, such as lawyers and real estate, are low.

12. The Netherlands has a strong licensing and registration framework for FIs, some VASPs and trust offices, which consists of robust checks to ensure criminals and their associates are prevented from operating in these sectors. However, while underground banking, unlicensed payment services and non-regulated providers of trust services are identified as high risk, there are insufficient resources allocated to mitigating these risks.

13. DNB and the Dutch Authority for the Financial Markets (AFM) have a good understanding of risk and apply a risk based approach, which is increasingly informed by robust data analysis. Understanding of risk by DNFBP supervisors is less developed and although some elements of a risk based approach are starting to be applied in some sectors, supervision is generally reactive and limited due to resource constraints. Despite two recent high profile out-of-court settlements involving major Dutch banks, some supervisors heavily rely on informal enforcement actions and warning letters. While informal measures can be

1 Dutch legislation allows the registration of senior managing officials as BOs. These are sometimes referred to as 'pseudo-BOs'. Pseudo BOs can be natural persons that belong to the senior management staff or the company, but can also be independent directors, or directors provided by trust offices that are senior management officials.

effective, they can also be slower to address significant issues, including unlicensed activity.

14. Most trusts cannot be established in the Netherlands (with the exception of Mutual Funds). Although nominee directors and shareholders are not recognised concepts in the Netherlands, they do exist in practice and are used in the management of conduit companies, which have no real presence in the Netherlands. Sanctions for failing to provide correct or up-to-date basic information are rarely imposed and no cases of providing incorrect BO information have been detected to date. At the time of the onsite, the Netherland's BO register was only 27% populated.

15. The Netherlands provides timely and constructive responses to mutual legal assistance (MLA) and extradition requests. Responses received by the FATF global network indicate that the provision of MLA is of high-quality, and properly prioritised. Simplified procedures within the European Union (EU) enhance co-operation with EU member states, which account for the vast majority of the Netherlands' MLA requests. The Netherlands' international co-operation on major international cases involving virtual assets (VA) is significant. However, pursuant to the international co-operation feedback received, the FIU-NL should seek a dialogue on how the quality of cross-border dissemination reports between EU FIUs can further improve their utility by recipient FIUs from the EU.

Risks and General Situation

2. The Netherlands is a financial centre with a large and globally interconnected financial system. It has one of the most concentrated banking sectors in the EU, with three Dutch banks controlling 82% of the sector's assets. Two of these banks have recently been part of a settlement with the office of the Public Prosecutor (OM) for significant AML/CFT failings and culpable ML and both banks have substantial presences abroad. The DNFBP sector includes approximately 162 TCSP providers in 2020, which are involved in activities including providing legal persons to manage the capital and business income of internationally operating companies, approximately 9 000 real estate agents and approximately 3 400 notaries and 790 notary offices. Notaries are required for most real estate transactions and incorporation of public or private limited-liability companies or the amendment of their articles of association, the formation of foundations or associations (including cooperatives). There is one state owned casino, approximately 4 000 dealers in precious metals and stone, who also trade in high value items such as watches and approximately 18 000 lawyers, although the authorities report that the majority of these do not carry out activities in scope of Dutch AML/CFT regulations. The Assessment Team therefore weighted most heavily the positive and negative aspects of supervision for FIs, as opposed to the DNFBP sector.

3. The Port of Rotterdam is the largest port in Europe and is vital for European import and export activities. This port acts as a gateway to Europe for people and goods, including significant volumes of illegal drugs, particularly cocaine from South America. A socio-cultural factor that is characteristic of the Netherlands is the culture of tolerance, in which tolerance with regard to soft[2] drugs has been identified by the Government as a contributing factor for the prevalence of drug crime and associated organised criminality.[3] Indeed, the Netherlands estimates that fraud and drug-related offences account for more than 90% of all Dutch proceeds of crime. Criminals use a variety of methods to launder their illegal proceeds, including licensed banks, dealers in high-value goods, intermediaries, purchasing real estate, or using companies or underground banking and unlicensed payment service providers. Terrorism related to religious extremism presents the main TF risk, but other terrorism threats exist, including right-wing terrorism.

Overall Level of Compliance and Effectiveness

Assessment of risk, co-ordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

4. Overall, the Netherlands has a good understanding of its ML/TF risks, as reflected in the NRAs and other sectoral assessments, policies, projects and cases. Many of the FIs and firms met by the Assessment Team were aware of the NRA's conclusions but noted that the NRAs and SNRAs are high-level policy documents that do not provide sufficient granularity on their specific sectoral risks. For example, the NRA does not provide a detailed assessment of the risks associated with the types of legal persons and arrangements in the Netherlands. National AML/CFT policies, strategies and activities generally seek to address the risks identified in the NRA, such as: risk-based thematic projects for criminal investigations; dedicated resources to countering organised criminal groups; and requiring payment service providers to make available all transaction data to the regulator.

5. The key strength of the Dutch system lies in its robust domestic co-ordination and co-operation on AML/CFT issues at both the policy and operational levels. The Netherlands is also seeking to explore and expand measures to intensify this domestic co-ordination. The Netherlands leverages a number of platforms to facilitate public-public, public-private and private-private partnerships to coordinate on AML/CFT and public-public partnerships to counter proliferation financing (CPF). There is room for improving the risk understanding, by including more relevant information in the NRAs. Some exemptions are inconsistent with the BES Islands' risk profile.

---

2 The *Opium Act* sets out the rules pertaining to drugs, and defines "soft drugs" as cannabis products (hash and marijuana), sleeping pills and sedatives. According to the government, these drugs carry less serious risks than hard drugs (e.g., heroin, cocaine, amphetamine, ecstasy and GHB) (see: www.government.nl/topics/drugs/difference-between-hard-and-soft-drugs).

3 NL ML NRA 2019-2020, p. 46.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

6. LEAs, including the Police and the Fiscal Information and Investigation Service (FIOD), have access to a broad range of financial intelligence and information to conduct their investigations into ML, TF and predicate offences and to trace criminal proceeds. Parallel financial investigations are a common practice for LEAs and OM. Datahubs such as iCOV, AMLC Suite, JustisTRACK, and the CT Infobox are a strong feature of the Dutch data-driven investigative model. Public-private partnerships, such as Financial Expertise Centre (FEC) including TF Task Force and the Serious Crime Task Force and the Fintell Alliance, as well as the close operational co-operation between FIU-NL and LEAs are additional strengths of the Dutch system to gather financial evidence, share best practices and discuss operational activities.

7. FIU-NL plays a major role in the production and dissemination of financial intelligence to LEAs, both proactively and upon request. It receives a significant amount of information from obliged entities on subjective and objective indicators. It has access to a large number of datasets, which allows it to enrich its analysis. These sources are an important added-value for the analysis performed by the FIU. FIU-NL's analytical products are of high quality and targeted to the needs of LEAs. In recent years, approximately 60% of FIOD investigations made use of STR information, and half of all TF investigations were triggered by FIU-NL's analytical products. The lack of comprehensive statistics on the usage of FIU disseminations in Police investigations and on the number of disseminations left unattended in the Police database is a minor concern, which is largely mitigated by the extensive co-operation between FIU-NL and LEAs and the frequent use of datahubs by the Police.

8. The Netherlands has a solid legal and institutional framework to investigate ML effectively. Financial specialists with the necessary expertise operate at both national and regional levels. There is sound co-operation and co-ordination between all competent authorities involved in ML investigations and combined teams merging police and FIOD expertise, are often deployed for complex investigations.

9. The Netherlands does not rely on the establishment of a predicate offence to investigate and prosecute ML. The authorities detect signals to initiate ML investigations from thematic projects involving all relevant authorities based on the NRA results, and on the national AML programme. The authorities do not maintain statistics on the types of ML and associated predicate offences investigated, prosecuted and convicted. However, case studies demonstrate that the authorities pursue a wide range of investigations, from self-laundering to complex cases, including offshore companies, professional money launderers and VAs, and that there is a general alignment between ML investigations and ML risks. Overall, the low level of sentencing for ML—including in some high-profile cases presented by the authorities—raises concerns on the dissuasiveness of the sanctions imposed for ML. ML investigations in the BES Islands mainly focus on predicate offences. While BES LEA expertise to conduct financial investigations has improved in recent years, the overall number of ML investigations and convictions remains low.

10. The Netherlands prioritises confiscation as a policy objective. Financial investigations into criminal assets and money-flows are a standard practice in all criminal investigations. Each LEA, as well as the OM, set annual seizure targets. Major multi-million confiscations imposed in out of court settlements involving legal persons account for the majority of the collected confiscation results. While not comprehensive, the statistics show that confiscation results are generally in line with the country's risk profile. The authorities actively pursue the tracing of VAs related to criminal activities as demonstrated by case studies, and the increasing amount of VAs seized annually. The Netherlands also pursues restitution, but no statistics are available.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

11. The Netherlands has a robust framework to detect, investigate and prosecute TF. The types of TF investigated and prosecuted are generally in line with the country's risks, with a majority of cases involving the funding to FTFs. However, the lack of any TF conviction for NPOs appears not in line with their high-risk categorisation in the TF NRA. The Netherlands also makes use of specific TF related public-public (FEC) and public-private TF Task Force (TFTF) partnerships. The authorities are aware of possible new emerging TF threats, such as right-wing terrorism. No TF case has been detected in the BES Islands, which is consistent with its TF risk profile. A CFT component is incorporated into the National Counter-Terrorism Strategy and the National Coordinator for Counterterrorism and Security cooperates closely with CFT authorities. The Netherlands has a good conviction rate in TF cases (70%), but the level of sentencing imposed is generally low. The Netherlands uses alternative measures where it is not possible to achieve a TF conviction, including alternative criminal charges, or administrative measures such as introducing community interventions at the local level.

12. The Netherlands implements TFS without delay, through a combination of EU and national provisions. Any new UN designation is immediately applicable in the Netherlands through a bridging provision, overcoming the delays with EU transposition. The Netherlands has a mechanism in place to identify targets for designation, and implements domestic designations pursuant to UNSCR 1373, in line with its risks. The communication of TFS lists to obliged entities may in some cases occur with delay. With the exception of trust offices, DNFBPs implementation of TFS without delay is not supervised. The same deficiency applies to DNFBPs in the BES Islands. This may impact their ability to implement TFS without delay.

13. The Netherlands has a robust understanding of the TF risks associated with the misuse of NPOs. Self-regulation is a key feature of the Dutch non-profit sector. The Netherlands has no supervisory authority to monitor NPOs and relies on voluntary certification mechanisms, such as the ANBI status and CBF seal, to promote transparency and accountability. The authorities have undertaken extensive outreach to the categories of good faith NPOs vulnerable to potential TF abuse. Good faith NPOs are aware of the risk of TF abuse, and are already implementing mitigating measures. The Assessment Team has some concerns as to whether the existing voluntary regulatory framework would be sufficient to detect bad faith NPOs[4] willingly sponsoring terrorism. The lack of supervision and transparency obligations for certain NPOs could be a challenge in detecting organisations raising funds without appropriate controls on the final beneficiaries or the intended use of the funds.

14. The Dutch authorities have a good understanding of contextual elements, risks and vulnerabilities linked to proliferation financing (PF). In particular, the authorities are aware of the possible exposure to PF, due to the country's position as a trade hub and its large financial sector, even if the overall risk is considered low. There is no supervision in place on the implementation of TFS obligations by DNFBPs other than trust offices. The Netherlands applies the same system in relation to TF, to implement PF TFS without delay, and the same issues relating to communication and supervision of the implementation of TFS obligations apply. Understanding of TFS obligations is strong in the financial sector, where DNB and AFM have provided guidance on sanctions implementation. In the absence of any supervision, it is unclear whether the DNFBP sector in the continental Netherlands, and DNFBPs in the BES Islands, are implementing TFS obligations at a satisfactory level.

Preventive measures (Chapter 5; IO.4; R.9–23)

15. FIs and VASPs demonstrate a strong understanding of their ML risks and obligations. DNFBPs have a reasonable understanding of ML risk. Understanding of TF risk is lower in all sectors. FIs and VASPs understand their CDD obligations, but the understanding of record-keeping requirements is varied. DNFBPs have a basic understanding of CDD and record-keeping requirements.

16. Some obliged entities find it difficult to determine BOs of complex structures, especially if these structures have international components. In these cases, obliged entities fall back on the legal option to identify pseudo BOs. Some DNFBPs rely on self-certification to identify BOs. However, they have limited options to verify this information and are unable to use the BO register as a source of information, given it is only partially populated. Implementation of EDD measures is generally comprehensive by FIs and VASPs. DNFBPs generally understand EDD obligations, but it is unclear how well these measures are applied in practice. Although most obliged entities were able to explain their obligations in relation to TFS, it was not clear if the DNFBPs implement TFS without delay, with the exception of trust offices, as most DNFBP supervisors do not review this as part of their supervision (see also IO.3).

[4] NPOs that deliberately give up tax advantages to avoid any transparency and accountability requirements linked to the voluntary certification systems, such as the ANBI status or CBF seal.

17. While obliged entities met by the Assessment Team generally understand and adequately implement their reporting obligations, it is not clear that this applies equally across all firms and sectors. For example, UTRs filed by some sectors, such as lawyers and real estate are low. Moreover, the overall quality of UTRs is unclear as there is little feedback provided by FIU-NL, other than to larger credit institutions (see also IO.6). Notaries are not able to submit UTRs until a business relationship has been established, which is inconsistent with other sectors and noted as a deficiency by the Assessment Team.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

18. In the financial sector, there are strong systems in place to assess the fitness and propriety of persons performing regulated activities. Many DNFBPs are not subject to licencing and registration, and where they are, it is often limited to professional body registration (e.g., Bar Association) and not fitness and propriety. The lack of access to BO information for most supervisors is a weakness. DNB and AFM have a strong understanding of sectoral risks and a robust risk model for categorising the risks of individual firms. Most DNFBP supervisors understand their sectoral risks. At the time of the onsite, some DNFBP supervisors were developing measures to improve risk understanding and help embed a risk-based approach to supervision.

19. DNB and AFM use a range of supervisory tools, including on and offsite supervision. DNB is harnessing data to deliver supervision more efficiently and this helped it respond to the challenges of the COVID-19 global pandemic. DNFBP supervisors use thematic investigations to some extent to address emerging issues. However, the frequency, scope and intensity of AML/CFT supervision and monitoring for DNFBPs is impacted by a lack of resources.

20. The recent high profile fines against two of the largest FIs in the Netherlands has had a significant impact on the prioritisation of AML/CFT compliance across the banking sector in particular. This has also had positive cascading effects in other sectors. While this is a noteworthy development, the duration of these AML/CFT failings suggests that previous actions were not sufficiently proportionate or dissuasive to change the culture within these large organisations and address long-term systemic AML/CFT failings. Some supervisors rely heavily on informal measures, such as warning notices, and do not use the full range of sanctions available to them in a consistent and proportionate way. A strength of the system is that in most cases remedial action plans are put in place and monitored by the regulators to ensure that issues have been addressed. The NRA highlights underground banking, unlicensed payment services and non-regulated providers of trust services as high risk for ML. However, the authorities do not currently allocate appropriate levels of resources to address these risks.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

21. The Netherlands has launched various initiatives aimed at identifying and assessing ML/TF risks of legal persons, but these do not provide a clear and coherent overview of these risks. Most trusts cannot be established in the Netherlands (with the exception of Mutual Funds). However, the Netherlands recognises foreign trusts and acknowledges there are a number in operation. The Dutch authorities do maintain information on foreign trusts holding real estate in the Netherlands. Supervision of TCSP also provides the authorities with some understanding of the types of investments the foreign legal trusts are engaged in.

22. All legal persons and other legal entities need to register basic information with the Chamber of Commerce (CoC) and most must also register BO information in the BO register. This information is publicly available, but currently the BO register is approximately 27% populated. The Netherlands mainly relies on FIs and DNFBPs to act as gatekeepers in order to mitigate the misuse of legal persons and arrangements for ML/TF. This is particularly important for notaries who play a key role in real estate transactions and company formation, and for the trust sector that service a large percentage of conduit companies for customers located in different jurisdictions seeking financial, tax, legal or other benefits.[5] While conduit companies are generally set up for legitimate financial tax or legal benefits, their international nature and often complex ownership structure makes it difficult to identify the ultimate BO, leading many obliged entities to settle for pseudo BOs (i.e., senior managing officials). This risk is intensified by the fact that 15% of trust services provided to conduit companies are offered by entities that have restructured their business models to circumvent stricter regulation (so-called “illegal trust offices”). The Dutch authorities recognise this problem, but are still struggling to identify solutions to address it, despite strengthening regulations in this area in 2018.

International co-operation (Chapter 8; IO.2; R.36–40)

23. In general, the Netherlands makes and responds to requests for international co-operation, aided by a broad range of international instruments, treaties and the use of Memorandum of Understandings (MoUs) which guarantee that legal and non-legal assistance is sought and provided to the fullest extent possible, and in line with risks. The centralisation of incoming/outgoing legal requests ensures that requests are tracked, prioritised and executed in a timely and coordinated manner. These legal requests are delivering results as evidenced through the numerous ML/TF case studies provided. Furthermore, feedback from the FATF global network on the Netherlands’ provision of MLA was generally positive.

24. Informal co-operation is facilitated through extensive networks of international Liaison Officers posted to jurisdictions based on risk. In particular, proactive assistance with EU member states is facilitated by a wide range of regional co-operation tools and information-sharing gateways, which streamline and expedite the process. This is an important feature as the majority of the Netherlands’ international co-operation is with other EU member states. FIU-NL actively cooperates at operational and strategic levels with a wide range of FIUs through the Egmont Group. Co-operation with European FIUs is robust with exchanges also occurring via the FIU.net.

25. In relation to FIU exchanges of cross-border dissemination reports, feedback from EU member states indicates that FIU-NL disseminations are numerous and that this type of disseminations can benefit from more context.

---

5 The term “conduit company” does not refer to the strict legal definition of conduit company in the Wtt 2018, but to companies with features that are typical for a conduit company. The relevant factors are whether a company has international structures, conducts transactions with related parties, has little or no real presence in the Netherlands, and has tax, financial or legal motives and/or substantial international money flows or balance sheet positions.

Priority Actions

1. The Netherlands should require all categories of DNFBPs and FIs, to take adequate measures to implement TFS without delay and to report frozen assets and ensure the implementation of TFS is supervised.
2. The Netherlands should take appropriate steps to ensure obliged entities, particularly notaries, take all reasonable measures to obtain and hold BO information and refuse their services when the ownership structure of their clients is so complex or opaque that they pose a genuine ML/TF risk.
3. Supervisory authorities should continue to make full use of the powers available and rely less on informal measures when significant AML/CFT violations are identified. All DNFBP supervisors should ensure they have appropriate enforcement policies so there is clarity when specific interventions should be applied.
4. The Netherlands should increase supervisory resources to improve risk-based supervision with varying levels of intensity. Resources should also be enhanced to tackle unlicensed activity, including underground banking and the provision of illegal trust services.
5. The Netherlands should enhance efforts to ensure the BO register is populated with accurate information on the BOs of legal persons active in the Netherlands and ensure that 'pseudo' BOs are only used in limited circumstances and not as an alternative to carrying out checks to identify ultimate BOs.
6. The Netherlands should further develop its understanding of the risks of conduit companies and take mitigating measures to reduce these risks. The Netherlands should also develop an understanding of the activities of foreign trusts operating within the jurisdiction and consider measures to mitigate risks in relation to high risk activities, such as real estate transactions.
7. The Netherlands should review the ML sentencing regime for natural and legal persons to ensure the penalties applied are sufficiently dissuasive and develop specific ML orientation points, including factors to consider when determining the penalty, based on the gravity of the offence. The OM should ensure that a larger and wider range of penalties is demanded in practice.
8. The Dutch authorities should amend BES legislation to address some technical deficiencies noted in the TC Annex. Moreover, BES LEAs should prioritise the investigation and prosecution of ML cases, in line with the risks and pursue stand-alone ML investigations.

Effectiveness & Technical Compliance Ratings

Table 1. Effectiveness Ratings

IO.1 - Risk, policy and co-ordination	**IO.2** International co-operation	**IO.3** - Supervision	**IO.4** - Preventive measures	**IO.5** - Legal persons and arrangements	**IO.6** - Financial intelligence
Substantial	**High**	**Moderate**	**Moderate**	**Moderate**	**High**
IO.7 - ML investigation & prosecution	**IO.8** - Confiscation	**IO.9** - TF investigation & prosecution	**IO.10** - TF preventive measures & financial sanctions	**IO.11** - PF financial sanctions	
Substantial	**Substantial**	**Substantial**	**Substantial**	**Moderate**	

Note: Effectiveness ratings can be either High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

Table 2. Technical Compliance Ratings

R.1 - assessing risk & applying risk-based approach	**R.2** - national co-operation and co-ordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
LC	**C**	**LC**	**C**	**LC**	**LC**
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
LC	**LC**	**C**	**LC**	**C**	**LC**
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
PC	**C**	**PC**	**LC**	**LC**	**LC**
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
LC	**C**	**LC**	**LC**	**LC**	**LC**
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
LC	**LC**	**C**	**LC**	**C**	**C**
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
LC	**LC**	**LC**	**LC**	**LC**	**LC**
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international co-operation		
C	**LC**	**LC**	**LC**		

Note: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC - partially compliant or NC – non compliant

MUTUAL EVALUATION REPORT OF THE NETHERLANDS

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 27 October to 18 November 2021.

The evaluation was conducted by an Assessment Team consisting of:

- Ms. Ohood AL BALUSHI, Central Bank of Oman, Oman (financial expert)
- Mr. Ichiyo OSAKI, Ministry of Finance, Japan (financial expert)
- Mr. Dieter PETRACS, Federal Ministry of the Interior, Austria (law enforcement expert)
- Ms. Cristina Schwansee ROMANO, Federal Public Prosecution Service, Brazil (legal/law enforcement expert)
- Mr. Werner VAN NOPPEN, Finance Ministry, Belgium (financial and sanctions expert)
- Mr. Shingo Yu-ho LAI, Hong Kong Police Force, Hong Kong, China (law enforcement and FIU expert)

The assessment process was managed by Ms. Kristen ALMA, Secretariat Team Lead, Mr. Ben ALDERSEY and Ms. Gaia MANSELLI, Policy Analysts, all FATF Secretariat. The report was reviewed by Mr. Juan Cruz PONCE (GAFILAT Secretariat); Ms. Shengnan YAN (China); and Mr. Carmine CARRELLA (Italy).

The Netherlands previously underwent a FATF Mutual Evaluation in 2011, conducted according to the 2004 FATF Methodology. The 2011 evaluation and 2013 and 2014 follow-up reports are published and available at www.fatf-gafi.org/publications/mutualevaluations/documents/mutualevaluationreportofthenetherlands.html.

That 2011 Mutual Evaluation concluded that the country was compliant with seven Recommendations; largely compliant with 20; and partially compliant with 22. The Netherlands was rated compliant or largely compliant with nine of the 16 Core and Key Recommendations.

In February 2014, the FATF recognised that the Netherlands made significant progress in addressing the deficiencies identified in the 2011 Mutual Evaluation Report and should be removed from the regular follow-up process. At that time, the Netherlands received re-ratings on all Core and Key Recommendations rated partially compliant in its 2011 MER.

Chapter 1. ML/TF RISKS AND CONTEXT

1

26. The Kingdom of the Netherlands is a parliamentary democratic constitutional monarchy consisting of continental Netherlands in Northwest Europe, three self-governing islands in the Caribbean (Aruba, Curaçao and Sint Maarten), and three smaller Caribbean islands, Bonaire, St. Eustatius and Saba (the BES Islands). Since 2010, the BES Islands are defined as public bodies (Dutch municipalities) of the Netherlands. Before this constitutional change, the BES islands formed part of the former Netherlands' Antilles. The self-governing Caribbean islands (Aruba, Curaçao and Sint Maarten) are subject to separate Mutual Evaluations by the Caribbean Financial Action Task Force and not considered as part of this MER. The BES Islands (Bonaire, St. Eustatius and Saba) are for the first time assessed and included in the Netherlands MER. Henceforth, the report will indicate specifically when the analysis refers to the BES Islands, whereas references to the Netherlands will imply continental Netherlands in Europe.

27. Continental Netherlands, with a population of 17.5 million, is bordered to the west and north by the North Sea, which separate it from the United Kingdom (UK), Denmark and Norway. It has land borders with Belgium and Germany. The BES Islands—with a population of 25 987 inhabitants in 2020 and a total surface area of 322 km^2—are situated in the Caribbean Sea.

28. The Netherlands is a founding member of the EU, and since 2002 its monetary unit is the euro (EUR). The BES Islands are not part of the EU and adopted the US dollar (USD) as its monetary unit. The Netherlands is the 17th largest economy in the world, with a GDP of EUR 810 billion in 2020, and the sixth largest economy in the EU.[6] The GDP of the BES was approximately USD 720 million in 2019, with tourism and salt mining as the main sources of income.

29. The Netherlands is a financial centre with a large and globally interconnected financial system. It has one of the most concentrated banking sectors in the EU, with three Dutch banks controlling 82% of the sector's assets. The financial sector is dominated by a small number of large national banks undertaking a wide range of activities (including one systemically important bank). The banking system comprises half the financial sector in terms of asset size.

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

30. The Netherlands' first NRA[7] was published in 2017, and a second published in 2020. The first NRA for the BES Islands was published in 2018, and a second published in 2021. In a separate study regarding the nature and scope on criminal expenditure in 2018, it was estimated that the volume of money laundered in continental Netherlands in 2014 was EUR 16 billion.

[6] World Bank, https://databank.worldbank.org/data/download/GDP.pdf, 2020.

[7] Separate NRAs were produced for ML and TF. These are referred to collectively.

31. In continental Netherlands, fraud[8] and drug related offences (including the production and sale of synthetic drugs) are considered major predicate offences, accounting for more than 90% of all proceeds of crime.[9] Domestic and international cases indicate that the proceeds of drug trafficking is often laundered through physical cash, often via the Port of Rotterdam and Schiphol Airport.[10] A socio-cultural factor that is characteristic of the Netherlands is the culture of tolerance, in which tolerance with regard to soft drugs are contributing factors for the prevalence of drug crime and associated organised criminality.

32. Theft, embezzlement, burglary and forgery are also common predicate offences. However, these account for significantly lower ML proceeds compared to fraud and drug-related offences. Criminals use a variety of methods to launder their proceeds, including licensed banks, dealers in high-value goods, intermediaries, purchasing real estate, or using companies or underground banking and unlicensed payment service providers.

33. The use of cash is relatively lower in the Netherlands than the rest of Europe. For example, in 2018, 37% of all purchases made by Dutch consumers were made in cash, while 63% was paid using a debit card.[11] However, as noted above, illicit proceeds related to drug trafficking is laundered using cash, and therefore remains a risk. The BES Islands have, to a large extent, a cash-based economy, which contributes to its ML risk profile.

ML through the financial system and shadow banking

34. As noted above, the Dutch banking sector is highly concentrated with three Dutch banks controlling most of the sector's assets. Two of these banks were recently subject to criminal investigations and significant out of court settlements for serious, systemic and long-term AML/CFT violations. Two of these institutions have substantial presences abroad. During the onsite visit, a third Dutch bank announced it was under-going a "punitive enforcement procedure", but it was unclear at that time if this procedure would result in a fine. As a result, the Assessment Team closely examined the contributing factors to these failings and the effectiveness of mitigation/remedial measures.

---

8 Fraud is a catch-all term covering many different forms of fraud, including tax fraud, social fraud and identity fraud.

9 NL ML NRA 2019-20, p.44 (English version).

10 For example, see www.eurojust.europa.eu/french-and-dutch-authorities-take-down-drug-trafficking-network-eurojust-support and www.dutchnews.nl/news/2020/05/police-find-e12-5m-in-cash-stashed-in-a-house-in-eindhoven/, NL ML NRA 2019-20, pp. 12, 18, 42.

11 Joint study by the Dutch Payments Association and De Nederlandsche Bank, see www.dnb.nl/actueel/algemeen-nieuws/oude-bulletins/dnbulletin-2019/dalende-trend-cash-zet-verder-door/. During the COVID-19 pandemic, cash payments dropped further to 13% of all payments, see www.dnb.nl/en/actueel/news-sector/sector-news-2021/payment-behaviour-during-the-pandemic/.

35. The NRA identifies Virtual Assets (VAs) as high risk for ML and TF in the Netherlands, given their relative anonymity. There is also evidence of criminal networks being increasingly active online (e.g., distributing drugs via the "darkweb") and using VAs in their illegal activities.[12] Furthermore, not all Virtual Asset Service Providers (VASPs) activities defined in the FATF recommendation are regulated in the Netherlands.

36. The Netherlands also identifies ML and TF by shadow banking—including the use of unlicensed payment service providers (PSPs) or intermediaries—as high risk. The Assessment Team therefore focussed on measures to address shadow banking, including hawala and unlicensed PSPs.

Offshore companies, legal entities and trust offices

37. The Netherlands has one of the highest global levels of incoming and outgoing foreign direct investment, including share capital and lending. At the end of 2018, Statistics Netherlands reported that the majority of incoming foreign investments was immediately channelled abroad via conduit companies. There are an estimated 12 000 conduit[13] companies in the Netherlands, with a balance sheet total of EUR 4 500 billion (550% of Dutch GDP).[14] Often the financial management and company's operations are located in a different jurisdiction and non-residents directly or indirectly participate or exert influence via share capital, including through trust offices. It is estimated that approximately 90% of conduit companies do not have their own staff in the Netherlands. A number of these entities are also used as holding companies with links to countries and regions with high levels of corruption[15] and can be used to channel money to offshore anonymous companies in jurisdictions with weak AML/CFT regimes. Complex structures with limited presence in the Netherlands can be used to disguise illicit funds and integrate them into the financial system due to the difficulties for gatekeepers in understanding the origin of assets and BOs. Conduit companies can also be created to facilitate tax evasion although various measures have been taken by the authorities to address tax base erosion and profit shifting to counter conduit companies and promote transparency and integrity. The Netherlands notes that unlicensed trust offices, in particular, are associated with ML risks related to offshore companies.[16]

Trade-based Money Laundering

38. The NRA identifies trade-based ML (goods and services) as a significant ML risk and there are cases where ML has been detected (e.g., in the context of a case of export of foodstuff to West Africa).[17] Accordingly, the Assessment Team considered efforts to detect and trace trade-based ML, including false invoicing and transactions.

[12] NL ML and TF NRAs 2019-20.

[13] The term conduit company used in this text is not a definition used in applicable Dutch legal instruments, but one that is used for statistical purposes.

[14] Government of the Netherlands, The road to acceptable conduit companies (2021).

[15] See: Corruption in the Great Lakes Region and Possible Ties to the Dutch Financial System (2020)

[16] NL ML NRA 2019-20, p.60.

[17] ML NRA 2019-20.

Real estate and DPMS

39. Transactions involving high value goods and real estate are also identified as high risk in the NRAs. Several cases indicate ML through purchasing high value goods and property, often through intermediaries.[18] Therefore, the Assessment Team considered the role of intermediaries including notaries and other legal professionals, DPMS, real-estate agents and FIs in undertaking adequate due diligence on higher risk transactions, the ability of law enforcement to obtain property ownership information and seize and confiscate assets.

Terrorist financing

40. The number of terrorist incidents in the Netherlands is low. Terrorism related to religious extremism (e.g., ISIL and other UN designated groups) presents the main TF risk in the Netherlands, but other terrorism threats exist, including right wing terrorism.[19] The TF NRA considers that terrorism in the Netherlands is largely self-funded through legal and illegal means, and is primarily used to finance family members in conflict zones. The highest TF risks were associated with the:

- acquisition and/or financing via foundations or other legal entities (charitable, religious, educational) established in the Netherlands and abroad,
- acquisition of and/or financing with legally obtained personal funds, and
- re-location via underground banking, including via unlicensed payment service providers.

BES Islands

41. The 2021 NRA for the BES Islands identifies the following ML risks: real-estate; use of physical cash; the formal and shadow banking sector (i.e., illegal money transfer businesses); falsification of company turnover and loan back constructions; misuse of front companies and misuse of legal arrangements; physical movements of cash (i.e., cash smuggling). The NRA also notes that due to the size of the islands, customers often know service providers personally, which may lead to a reluctance to apply stringent CDD measures or report unusual transactions to FIU-NL. The NRA notes that Bonaire is a transit point for drugs to Europe from Latin America, and the BES Islands can be used as transit and final destinations for human trafficking.

Areas of lower ML and TF risks and focus

42. The Transparency International Corruption Perception Index identifies the Netherlands as having relatively low levels of domestic corruption.[20] Therefore, the Assessment Team de-prioritised the laundering of illicit proceeds from domestic corruption.

18 ML NRA 2019-20, p. 52 (English version).

19 NL Terrorism Threat Assessment, April 2021, https://english.nctv.nl/topics/terrorist-threat-assessment-netherlands/documents/publications/2021/04/26/terrorist-threat-assessment-for-the-netherlands-54.

20 Transparency International, Corruption Perceptions Index, www.transparency.org/en/cpi/2020/index/nld, 2020.

43. Concerning TF, the Dutch authorities noted in the BES NRAs that there are no indications of the existence of threats relating to terrorism or TF in the BES Islands. The risk and materiality of the various sectors in the BES Islands were also weighted accordingly throughout the MER.

Materiality

44. The Netherlands is the 17th largest economy in the world, with a GDP of EUR 810 billion in 2020, and the sixth largest economy in the EU.[21] The GDP of the BES was approximately USD 720 million in 2019. The Netherlands is the fifth largest exporter of goods in the world (after China, US, Germany and Japan) and the sixth largest exporter of commercial services. Currently, almost two-thirds of the economy is based on foreign trade, primarily with Germany, Belgium, UK and France.

45. The financial sector is dominated by a small number of large national banks undertaking a wide range of activities. The banking system comprises half the financial sector, in terms of asset size.

46. During the financial crisis, the government bailed out a limited number of banks and remains part owner of one bank and full owner of another bank. The pension system is ranked first globally by share of GDP and the insurance sector has consolidated assets amounting to around 140% of GDP. The financial sector contributes 7% to the overall GDP.

Structural Elements

47. The Netherlands has all of the key structural elements required for an effective AML/CFT system, including political and institutional stability, a high-level commitment to address AML/CFT issues across various parts of government, governmental accountability, rule of law, and a professional and independent judiciary.

Background and Other Contextual Factors

48. In 2017, the World Bank reported that 100% of the adult population in the Netherlands held a bank account.[22] In 2020, migrant remittance outflows and inflows totalled just over EUR 13.9 billion and EUR 2.5 billion respectively.[23]

AML/CFT strategy

49. The government launched a ML Action Plan in June 2019, which is comprised of three main pillars, and includes initiatives such as enhancing transparency of legal persons and arrangements, a prohibition on cash transactions over EUR 3 000 for dealers in goods, regulation of VAs, strengthening the AML/CFT framework in the BES Islands; increasing effectiveness of supervision, and strengthening investigation, prosecution and the confiscation of criminal assets. This Plan is supported by a series of programmes, such as the confiscation of criminal assets initiative, and increased financial support for FIOD, the Anti Money Laundering Centre (AMLC).

---

21 World Bank, https://databank.worldbank.org/data/download/GDP.pdf, 2020

22 World Bank, Global Findex Database, 2017.

23 World Bank, Migration and Remittances Data (worldbank.org)

50. In September 2020, the Minister of Finance and the Minister of Justice and Security issued a TF Policy Statement 2020 to the Parliament in response to the TF NRA 2019. This Statement refers to existing measures taken to mitigate risks related to TF via foundations or other legal forms, to TF using underground and hawala banking, and the movement of cash and TF via VAs.

51. Regarding CPF, in 2020, the Netherlands conducted an initial risk assessment, the "Proliferation Financing Policy Monitor". The authorities consider the threat of PF sanction evasion to be insignificant due to the limited financial flows with Iran and DPRK, and the implementation of PF sanctions at the EU and Dutch levels.

Legal & institutional framework

52. AML/CFT policies and activities in the Netherlands are characterised by strong co-operation between competent authorities, as well as with the private sector. The Minister of Finance shares responsibility for the AML/CFT policy with the Minister of Justice and Security. The primary authorities responsible for AML/CFT are outlined below:

- The **Ministry of Finance** coordinates the prevention of ML, TF, and PF and ensures the implementation of the laws relevant for the proper operation of the financial markets. The Ministry also oversees the AML/CFT supervisors for the financial markets and some DNFBPs.

- The **Ministry of Justice and Security** is responsible for legislation related to civil, administrative and criminal laws and procedures. The Ministry is also responsible for the Police, OM, and FIU-NL, as well as some DNFBP supervisors.

- The **National Coordinator for Counterterrorism and Security** (NCTV) falls under the responsibility of the Minister of Justice and Security and is responsible for policy development, analysis of intelligence and other information as well as co-ordination of counter-terrorism measures.

- The **Ministry of Foreign Affairs (MFA)** coordinates and carries out Dutch foreign policy, including the implementation of UN and EU sanctions.

- The **Chamber of Commerce (CoC)** falls within the Ministry of Economic Affairs and Climate and maintains the commercial register, including a BO Register.

- The **Netherlands Police (Police)** is the national police force comprised of ten regional units, and a Central Unit. All regional units feature a financial investigation team on AML/CFT and teams specialising in terrorism (including TF). The BES Islands have their own Dutch Caribbean Police Force (KPCN), which can be supported in large investigations by the Netherlands Police and the police from Aruba, Curacao and Sint Maarten. The Detective Co-operation Team (RST) is a partnership of police forces from all jurisdictions within the Kingdom, in charge of serious cross-border offences across the Netherlands, Aruba, Curacao, Sint Maarten and the BES.

- The **Financial Intelligence Unit** (**FIU-NL**) is located within the Netherlands Police, and is operationally independent and autonomous. FIU-NL is the national centre for receiving, analysing, and declaring suspicious transaction reports, which are disseminated to LEAs. The FIU-NL is also responsible for the BES Islands, where it has stationed an officer.

- The **Public Prosecution Service (OM)** independently decides whether to prosecute a case and on how to deal with certain categories of crimes without going to court. The OM ensures that criminal offences, including ML and TF are detected and prosecuted and cooperates with the Netherlands Police and other investigation services, such as the Fiscal Intelligence and Investigation Service (FIOD). The OM BES operates in the BES Islands and forms part of OMCarib (which includes Curaçao and Sint Maarten). OM BES also has one specialised prosecutor for ML investigations.

- The **Fiscal Information and Investigation Service (FIOD)** falls under the responsibility of the Ministry of Finance and is responsible for investigating fiscal and financial crimes, including ML and TF.

- The **Tax and Customs Administration** is part of the Ministry of Finance and, *inter alia*, is responsible for supervising the transit of goods and currencies and has AML/CFT as one of its key tasks. The Caribbean Netherlands Tax and Customs Administration (BCN) is responsible for the BES Islands.

- The **Royal Netherlands Marechaussee (KMar)** falls under the Ministry of Defence and is responsible for both national and Schengen border control, participates in Cost Guard Agency Frontex and investigates migration and border related crimes in co-operation with Customs and FIOD.

- **De Nederlandsche Bank** (**DNB**) is the independent Dutch central bank and acts as the prudential supervisor for the financial sector and AML/CFT and Sanctions Act supervisor for banks, pension funds, insurers, payment institutions, foreign exchange offices, electronic money institutions, virtual asset service providers (since 2020), and trust offices. In addition, DNB supervises the institutions that mainly engage in the performance of one or more activities listed under points 2, 3, 5, 6, 9, 10, 12 and 14 of Annex of the Capital Requirement Directive. For example granting loans, factoring, financing of commercial transactions, custody and management of securities and safe custody services. On the BES Islands, DNB is the AML/CFT and Sanctions Act supervisor for the same categories of institutions. In addition, DNB is the AML/CFT and Sanctions Act supervisor for casinos on the BES.

- The **Dutch Authority for the Financial Markets (AFM)** is responsible for supervising AML/CFT compliance by (managers of) alternative investment funds, (managers of) undertakings for collective investment in transferable securities, investment firms and financial service providers providing intermediary services in life insurance contracts. In regard to the Sanctions Act, the AFM supervises the compliance by the managers of alternative investment funds and undertakings for collective investment in transferable securities as well as investment firms. In the BES Islands, AFM is the supervisor for AML/CFT compliance and compliance with the Sanctions Act for all of the above categories of institutions.

1

53. The main public-public and public-private co-operation bodies are summarised in the below table:

Table 1.1. Primary domestic co-operation bodies (including public-private partnerships)

Name	Public-Public or Public-Private	Description
Financial Expertise Centre (FEC)	Both	Permanent AML/CFT body for supervisory, investigative and enforcement agencies. FEC Structural programs involving public-public and public-private also exist, on TF as well as serious crimes.
Anti-Money Laundering Centre (AMLC)	Both	Is a platform where all parties, both public and private, involved in AML share their knowledge and experience and work together on operational matters.
Steering Team Money Laundering	Public-Public	Assesses whether LEA signals qualify for ML investigation.
Steering Team on Supervision	Public-Public	Makes *una via*[24] decisions, in close co-operation with DNB and AFM, on cases involving punitive enforcement measures.
The Regional Information and Expertise Centres (RIECs) and the National Information and Expertise Centre (LIEC)	Public-Public	Work at a regional level to link up the information, expertise, and powers of government bodies, including the municipal authorities, the provincial authorities, and various LEAs on organised crimes including ML investigations.
The Obliged Entities Committee	Public-Private	Coordinating partnership to discuss (proposed) legislation and policy plans related to UTRs.
AML/CFT Supervisors Committee	Public-Public	The six AML/CFT supervisors (and MoF, MoJ&S and FIU-NL) frequently meet to discuss cases and case law and consult one another to achieve AML/CFT supervisory convergence.
TF Platform	Public-Private	Initiative of the Dutch Banking Association and FIU-NL to share knowledge of themes, phenomena and typologies with the four Dutch major banks.
Asset Freezing Committee	Public-Public	The consultations address both the implementation of TFS and the placement of suspected terrorists and terrorist organisations on the National Terrorism Sanctions List.
Carré Consultations	Public-Public	Headed by MoFA to discuss export controls to prevent the proliferation of weapons of mass destruction (including sanctions evasion).
Sanctions Act Consultation Meeting	Public-Public	Discusses the legal aspects of implementing sanctions and sanction Acts with multiple government organisations
Sanctions Expert Pool and International Sanctions Network	Public-Private	Sanctions Expert Pool organised by the Dutch Banking Association, is a forum for banks and DNB to discuss the execution of sanction measures and to share best practices. MoF facilitates a similar meeting of all non-bank FIs (the International Sanctions Network).
Fintell Alliance	Public-Private	A public-private partnership with four major banks to exchange financial intelligence and knowledge to improve the efficiency and efficacy of UTRs.

Financial sector, DNFBPs and VASPs

54. This section provides general information about the size and composition of the FI and DNFBP sectors in the Netherlands. FIs and DNFBPs are not of equal importance given their role and size, and their different levels of exposure to ML and TF risks. The level of risk also varies greatly between individual FIs and DNFBPs within the same sector. The Assessment Team ranked the sectors based on the relative importance, materiality and the level of risk. These rankings have been used to weight positive and negative implementation issues throughout the report, as a basis for conclusions.

[24] Whereby it is impossible to impose both criminal and civil/administrative sanctions for the same offence.

Overview of Financial Sector

55. **Banking sector:** is weighted as the most important in the Dutch context, reflecting the size of the sector, and its exposure to ML/TF risks, and the recent significant and long-term AML/CFT violations identified. At the end of September 2021, 84 banks or branches of banks from Member States or third countries were active in the Netherlands. The total balance sheet of all banks amounted to EUR 2 780 billion in Q3 2021, with three banks holding more than 80% of the balance.

56. **MVTS:** is weighted as important in the Dutch context, reflecting the diversity of the population, not only in size and transaction volume, but also in services, channels and geographical activity, all of which expose it to ML/TF threat. The sector includes mobile and internet-based payment systems, digital wallets, electronic money, money transfer offices (MTOs) and alternative banking platforms. This sector continues to grow, both in number of institutions and transaction size. For example, in 2019, the market for licensed payment institutions and electronic money institutions grew by almost 50%. There are also a number of underground payment service providers in the Netherlands. With the passage of the EU Payment Service Directive, the number of locations where a money transfer can be carried out in the Netherlands has increased to more than 900 locations, including approximately 818 agents operating on behalf of foreign MVTS providers.

57. **VASPs:** is also weighted as important in the Dutch context. The NRAs identify VAs as high risk for ML and TF. Not all VASPs activities defined in the FATF Standards are currently regulated in the Netherlands. As of 18 November 2021, 65 VASPs have applied for mandatory registration to operate in the Netherlands, 25 VASPs have been registered by DNB and nine applications are being processed (including two expansions).[25]

58. **Asset Management:** is weighted as moderately important in the Netherlands. This is the second largest asset management sector in Europe and includes the broader securities sector and investment management activities such as managing alternative investment funds, managing of undertakings for collective investment in transferable securities (UCITS). In 2019, the Netherlands held the second largest foreign investment stock in Africa after France, although more than two thirds of those investments were in Egypt, Nigeria, and South Africa. At the end of 2019, investment funds managed EUR 899 billion in assets and investment firms managed EUR 249 billion in assets. Approximately 90% of the managed assets of investment firms come from professional clients and 10% from retail investors.

59. **The insurance and pensions sectors:** are weighted as less important in the Netherlands context, due the low inherent ML/TF risk. In 2019, the insurance sector was composed of a total of 136 insurers. This includes life insurers, which are subject to AML/CFT regulation. The insurance sector is diverse. Based on premium volumes, the health insurance sector is by far the largest in the Dutch insurance market with premium volumes in excess of EUR 52 billion. Life and non-life insurance (excluding health insurance) both represent approximately EUR 13 billion in premium volume. The Netherlands has one of the world's most highly developed pension fund industries, with total private assets managed being amongst the highest in Western Europe. The value of the pension funds' equity and debt portfolios was EUR 1 560 billion at the end of 2019.

[25] 26 have withdrawn.

60. **BES Islands:** The financial sector in the BES is very small, with financial services sector comprising 10.4% of the economy in Bonaire, and less than 5% in both Saba and St. Eustatius.[26] In total, in 2020, there were 10 credit institutions offering services in the BES Islands.

Overview of DNFBP Sector

61. **Trust company and service providers (TCSPs)**: the TCSP sector is weighted as important in the context of the Netherlands. The Dutch NRAs note that *unlicensed* trust offices are associated with significant ML risks. The Dutch TCSP sector in 2020 was comprised of 162 licenced trust offices and an estimated 600 domicile providers. The services provided by a trust office include acting as director of a legal person or company and the provision of a postal address, combined with the provision of certain specific administrative services (the latter is referred to as 'domicile plus'). Trust offices are regulated by the Trust and Company Service Providers Supervision Act 2018 (Wtt 2018) in as far as CDD and ethical business operations are concerned and are regulated by the Money Laundering and Terrorist Financing Prevention Act (Wwft) for AML/CFT obligations. A trust office may, for the benefit of a customer, use a legal person or company that is part of the trust office for managing the capital and business income of an internationally operating company. The provision of a postal address not combined with certain specific administrative services (referred to as 'domicile sec'), is a service that is covered by the Wwft and the providers are described as domicile providers. Domicile provision without certain specific administrative services is a lower risk activity than those provided by trust office or domicile plus.

62. **Real estate agents:** are weighted as moderately important in the Dutch context. Transactions involving real estate (including through loan back arrangements, ABC supply chain transactions, offshore companies and trusts) are identified as a significant ML risk. However, real estate agents are not involved in all transactions. There are approximately 9 000 real estate agents in the Netherlands and some real estate is held by foreign trusts, which do not need to be registered as such in the Netherlands.

63. **Notaries:** are weighted as moderately important in the context of the Netherlands. Around 3 400 civil-law notaries (776 firms) have been appointed by the Ministry of Justice and Security and they are required to be members of the Royal Dutch Association of Civil-law Notaries (KNB). Dutch law requires a notarial deed for a number of agreements and legal transactions, including real estate transactions and the incorporation of all private legal entities, with the exception of church communities. This makes notaries key gatekeepers, particularly in higher risk areas such as real estate transactions in the continental Netherlands and BES Islands. Notary trust accounts in the Netherlands are estimated to hold over EUR six billion each day.[27]

---

[26] Centraal Bureau voor de Statistiek, "Trends in the Caribbean Netherlands", 2019, www.cbs.nl/en-gb/publication/2019/51/trends-in-the-caribbean-netherlands.

[27] Onvolledige dossiers en weinig controle op witwassen: kwart notariskantoren heeft zaakjes niet op orde

64. **Lawyers**: are weighted as moderately important in the context of the Netherlands. There are approximately 18 000 lawyers in the Netherlands (5 600 firms), some of which are involved in company formation and real estate transactions. According to the Netherlands Bar (NOvA), in 2020 only 28% of the lawyers and only 22% of the law firms were involved in AML/CFT services. All lawyers are required by law to be a member of the Bar Association.

65. **Dealers in precious metals and stones (DPMS):** are weighted as moderately important in the Netherlands context. DPMS is regulated for AML/CFT when cash payment exceeds EUR 10 000. There are approximately 4 800 DPMS in the Netherlands.[28]

66. **Accountants:** are weighted as moderately important in the Netherlands. Some 8 800 public accountants (as opposed to in-house accountants) are active in the Netherlands. Of the total number of public accountants, 4 600 are registered accountants. In addition, there are about 4 200 accounting consultants. An accounting consultant is an internationally recognised accountant authorised to perform audits.

67. **Casinos:** are weighted as being of lower importance in the context of the Netherlands. There is only one licensed casino in the Netherlands (with multiple branches), which offers croupier-serviced betting games over EUR 3 000. This casino is state-owned and its managing and supervisory boards are appointed by the Minister of Finance. The gross revenue of the company amounted to EUR 729 million in 2019. Amusement arcades, which sometimes advertise as "casinos", may only operate slot machines for small bets and are exempt from AML/CFT supervision due to their perceived low risk. As of 1 October 2021, the Netherlands began regulating online casinos (including supervision for AML/CFT), with 10 licenses provided by 18 November 2021.[29]

68. **BES Islands:** The DNFBP sector is very small and poses a relatively small risk compared to continental Netherlands. Most DNFBPs present in the BES Islands (80 in total) fall under the supervision of the BTWwft. The one trust office and the two casinos present are considered low risk and are supervised by DNB. Risks relating to real estate are high, particularly in Bonaire.

Preventive measures

69. The Netherlands is a member of the EU, and therefore bound by EU law. EU AML/CFT Regulations directly apply in the Netherlands (excluding the BES Islands), and EU AML/CFT Directives are transposed through Dutch domestic law. The main elements of EU legislation, including AML Directives, have been implemented in the Money Laundering and Terrorist Financing (Prevention) Act (Wwft). This law was most recently amended by the Fifth Anti-Money Laundering Directive (Amendment) (Implementation) Act, which entered into force on 21 May 2020.

---

[28] A wider range of dealers or brokers in high-value goods are subject to supervision in the Netherlands than prescribed by the FATF. For instance, dealers and brokers in vehicles (e.g., cars), vessels (e.g., yachts), art and antiques, jewellery, furniture and kitchens are also supervised.

[29] The AML/CFT regulation of online casinos extends to activities that are not regulated for physical casinos, such as sports betting and horse racing.

70. In addition to the Wwft, there are several other laws in the Netherlands containing AML/CFT elements, notably:

- Financial Supervision Act (Wft): deals with the supervision on banks, insurance companies and other FIs;
- Criminal Code (WvSr): establishes criminal offences under Dutch law, including ML and TF;
- Code of Criminal Procedure (WvSv): outlines criminal justice procedures and powers of LEAs;
- Sanctions Act: provides the basis for international and national freezing measures and other sanctions, and for supervision of compliance with sanction regulations.
- Trust and Company Service Providers Supervision Act (Wtt 2018): includes the primary preventive measures for trust offices; and
- Economic Offences Act: criminalises breaches of legislation prescribing preventive measures in the field of AML/CFT.

Legal persons and arrangements

71. Most legal persons in the Netherlands, are established through a notarial deed for an indefinite period of time. All types of legal persons and other legal entities are required to register with the Dutch CoC. In September 2020, the CoC started operating a public BO Register for legal entities. Foreign legal entities are registered with the CoC if they have a branch or commercial undertaking in the Netherlands. As of 18 November 2021, a total of about 1.93 million Dutch and 9 000 foreign and European legal entities were registered with the CoC. Approximately 67% of all private legal persons registered in the CoC are private limited liability companies. In 2020, there were approximately 6,200 legal persons registered in the BES Islands. Approximately 2335 of these were Private Limited Liability Companies, 200 were foreign entities and 1800 sole proprietorships.

Table 1.2. Number of legal entities registered as of 15 November 2021[30]

Description	Number	Basic characteristics	Legal personality
Private limited liability company (BV)	1 121 871	BVs may be set up by one or more natural or legal persons and are managed by one or more directors, which are elected by the shareholders. Any powers not conferred upon the directors remain vested in the general meeting of shareholders. BVs may issue only registered shares. BVs have an obligation to register the transfer of shares within the company and to have such a transfer certified by way of notarial deed.	Yes
Foundation	266 109	Foundations have no members and their purpose is to realise a (charitable) objective. While profits are not excluded, there are strict restrictions in place concerning the effective allocation of these profits. A foundation is established by notarial deed.	Yes
General partnership (VOF)	193 736	This a partnership in which two or more partners cooperate in the exercise of their business (e.g., contractors).	No
Association	131 676	An association is a partnership between two or more members to achieve an objective, which can include profits. However, profits may be used only to further the common goal and may not be distributed to its members. Associations have full legal personality and are set up by notarial deed and required to register with the CoC.	Yes
Association of proprietors	128 071	Members are owners of apartments within an apartment building, with the objective to act in their common interest in regard to the building, such as maintenance. Membership is mandatory.	Yes
Professional Partnership	37 763	This is a partnership in which two or more professionals join activities for a common purpose (e.g., cooperating doctors, lawyers, etc.). Partners are in equal parts liable for debts arising out of legal acts engaged upon by each of them on behalf of the partnership.	No
Limited partnership (CV)	11 628	This is a partnership where a company is operated in a manner visible to third parties. In this respect it is similar to the general partnership. However, there are one or more silent partners that provide capital and are only liable to the extent of their investment. In exchange for their limited liability, the silent partners are not allowed to engage in legal acts on behalf of the partnership.	No
Cooperative	9 417	Cooperatives are legal entities in which a number of persons combine their resources to facilitate their individual but similar interests. Cooperatives may be established by two or more members through a notarial deed. A Cooperative has no minimum capital requirement and cannot issue any shares or certificates.	Yes
Church Community	7 369	Church communities are religious legal persons governed by their own articles of association and do not require notarial deed.	Yes
Public limited liability company (NV)	4 935	Public limited liability companies (NV) are subject to the same establishment requirements, and closely follow the ownership and management structure, of the private limited liability company (BV). Dutch NVs require a minimum capital (EUR 45 000) and NV-shares may be publicly traded	Yes
Public legal person	5 767	Public entities such as the State, provinces and municipalities.	Yes
Mutual insurance company	247	Mutual insurance companies are associations for insurance purposes.	Yes
Shipping company	125	Used when a ship has multiple owners for the purpose of exploitation of the ship.	No
European Economic Interest Grouping	58	European form of partnership in which companies or partnerships from different European countries can cooperate. Partners are jointly and severally liable.	No
European Company (SE)	35	SEs are subject to the same registration requirements as NVs.	Yes
European cooperative society (SCE)	2	SCEs are subject to the same registration requirements as NVs.	Yes

Source: Chamber of Commerce

[30] This does not include legal entities incorporated in the BES Islands.

72. Dutch law does not provide for the establishment of legal arrangements, such as express trusts. However, express trusts established under the laws of another country are recognised. The Dutch authorities estimate that there are up to 15 000 legal arrangements, including foreign legal arrangements, in operation in the Netherlands.

73. There is one Dutch legal arrangement, referred to as a "mutual fund", which shares similarities with a trust, in the sense that it is a freeform contractual arrangement often used for some form of asset management, with the important distinction that it has transferable participant certificates. The mutual fund has two variants: the open fund and the closed fund. As of 2020, there are approximately 2 800 open mutual funds in the Netherlands. The open fund is primarily used as an investment fund, as it allows a number of participants to deposit capital to be invested for their mutual benefit. These investment funds require a license to operate. Since open and closed mutual funds do not have legal personality, have no rights or obligations other than certain tax advantages (open funds are held to pay corporate tax), no procedural requirements apply to their creation.

Supervisory arrangements

74. There are six independent AML/CFT supervisors for different groups of obliged entities. The supervisors for FIs are DNB and AFM. Concerning the BES Islands, DNB supervises FIs, TCSPs and casinos, and the AFM supervises life insurance intermediaries. VASPs are not regulated in the BES islands. The below table summarises their respective responsibilities for AML/CFT supervision, as well as the number of entities under their responsibility.

75. DNB employs in 2021 60 staff dedicated to AML/CFT supervision, and the AFM employs 13 staff members dedicated to AML/CFT supervision. These figures include AML/CFT supervision for the BES Islands.

Table 1.3. Supervisory authorities for FIs in the Netherlands in 2020

FI Sector	Supervisor	Number of FIs
Banks, including non-EU branches	DNB	84
Payment Institutions (including MVTS, foreign exchange offices and electronic money institutions)	DNB	60
Insurers (including life insurance companies)	DNB	91
VASPs	DNB	15
Investment firms (licensed)	AFM	308
Managers of investment institutions, including UCITS (licensed)	AFM	109 (of which 14 managers of UCITS)
Managers of investment institutions (registered, unlicensed)	AFM	478
Intermediaries of life insurance	AFM	4 473

76. The supervisors for the DNFBP sectors, other than DNB, are the Financial Supervision Office (BFT), Tax and Customs Administration AML/CFT Supervision Office (BTWwft), Netherlands Gambling Authority (Ksa) and the Deans of the Netherlands Bar (NOvA). The below table summarises their respective responsibilities for AML/CFT supervision, as well as the number of entities under their responsibility.

77. The **BFT** is the independent AML/CFT supervisor of (junior) civil-law notaries, public (chartered) accountants, business administration consultants, tax advisors and other independent financial economic or legal advisers. The BFT employs 15 staff members dedicated to AML/CFT supervision. The BFT has supervisory arrangements with professional bodies or organisations, including the Dutch Register of Tax Advisers (RB) and the Association of Registered Accountants (SRA), which peer review or audit their own members.

78. The **BTWwft** is responsible for the AML/CFT monitoring of traders or brokers in high-value goods, including DPMS and dealers or traders yachts, cars, art and antiques, as well as real estate brokers, real estate valuers, pawnbrokers, and natural or legal persons that provide street or postal addresses in a professional or commercial capacity (domicile providers). In addition, BTWwft supervises all DNFBPs on the BES Islands (except for one trust office and two small casinos, which are supervised by DNB). BTWwft employs approximately 41 staff members dedicated to AML/CFT supervision.

79. The **Ksa** is the supervisor of games of chance in the Netherlands. In 2016, the Ksa took over the AML/CFT supervision of casinos from DNB. The Ksa employed one AML/CFT supervisor until 2021, but has now increased its number to three due to Ksa taking on supervision of online gambling.

80. **NOvA** is the professional organisation of the legal profession. The local bar presidents of the 11 districts and their staff members (approximately 125) and eight staff members of the NOvA act as supervisors of the legal profession. As of July 2021, one of the Deans was appointed to supervise lawyers in the BES Islands.

Table 1.4. Supervisory authorities for DNFBPs in the Netherlands in 2020

FI Sector	Supervisor	Number of DNFBPs
Casinos	Ksa	1 (including 14 branches)[31]
Real estate agents	BTWwft	9 000*
Traders in high-value goods (including dealers in precious metals and stones)	BTWwft	90 200 (DPMS is 4 800*)
Lawyers	NOvA	18 000
Notaries (individuals)	BFT	3 382[32]
Accountants	BFT	9 064
Tax advisors and independent legal professionals	BFT	25 000*
TCSP - Trust offices	DNB	162
TCSP - Natural or legal persons that provide street or postal addresses in a professional or commercial capacity (domicile provider)	BTWwft	600*

Note: These figures are estimates by the authorities.

International co-operation

81. The Netherlands makes and responds to requests for international co-operation, aided by a broad range of international instruments, treaties and the use of Memorandum of Understandings (MoUs) which guarantee that legal and non-legal assistance is sought and provided to the fullest extent possible.

82. MLA requests are centralised for non-EU countries through the Department of International Legal Assistance in Criminal Matters (AIRS) of the Ministry of Justice and Security, prior to referral to International Legal Assistance Centres (IRCs). An IRC is a co-operation between the OM and LEAs and consists of one or two prosecutors, administrative staff and police officers. For EU states, requests are sent directly to and from IRCs. The centralisation of MLA requests ensures that requests are tracked, prioritised and executed in a timely and coordinated manner.

83. Since 2016, more than 20 000 MLA requests were received annually by the Netherlands, and over 13 000 requests were sent to foreign counterparts. About 85% of the incoming requests come from EU member states. Within the EU most requests between 2015 and 2019 came from Belgium, Germany, France and Poland. Outside of the EU, the most frequent incoming requests are from the United Kingdom, Switzerland, Turkey, the United States and Norway. Outgoing MLA requests are sent mostly to EU member states (75%), primarily to Belgium, Germany, Poland, Spain and France. Outside of the EU, the Netherlands most frequently sends MLA requests to the United States, Turkey, Surinam, Switzerland and Morocco.

84. The Netherlands initiates and takes part in Joint Investigative Tools (JITs), but there is no legal basis for the establishment of JITs in the BES Islands.

[31] Online casinos have been regulated since October 2021 and there were 10 licensed online gambling sites at the time of the onsite.

[32] As of 1 October 2021.

Chapter 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION

Key Findings and Recommended Actions

Key findings

1. Overall, the Netherlands has a good understanding of its ML/TF risks, as reflected in the NRAs, SNRAs and other sector assessments, policies, projects and cases. The methodology of the NRAs is general sound and based on a structural process to collect and evaluate qualitative inputs from policy, supervisory, law enforcement and private sector authorities through extensive surveys, meetings and interviews. However, inputs into the NRAs can be strengthened by the inclusion of additional quantitative sources.
2. In continental Netherlands, fraud and drug related offences account for more than 90% of all proceeds of crime and ML risk manifests via the use of crypto currencies; trade-based services; underground banking, including unlicensed payment services; offshore companies; and services/goods of dealers of high-value goods. The TF NRA considers that terrorism in the Netherlands is largely self-funded through legal and illegal means, and is primarily used to finance family members in conflict zones.
3. For the BES Islands, the authorities have a less informed but adequate understanding of the islands' ML/TF risks as outlined in the BES NRAs. According to the NRA, the highest ML risk lies in the real estate sector, in particular large cash transactions. The NRAs briefly touch upon TF, but do not include a detailed assessment, as there were no authorities who were aware of any indication of terrorism or TF in the BES Islands.
4. The ML risks identified seem reasonable and align with input received from FATF and FSRB members. The authorities could further strengthen this understanding by building upon the risks related to methods and channels, considering the ML risks associated with the underlying predicate offences including the origins of proceeds, and expanding the categorisation of the risks of different FI and DNFBP sectors compared to each other at the national level.
5. TF risks are well identified and understood. This understanding is supported by knowledge, projects and cases developed by the FIU-NL, OM and LEAs, coupled with the on-going terrorism threat assessments conducted by the intelligence agencies involved in counter-terrorism.
6. FIs, DNFBPs and NPO sector representatives met by the Assessment Team had a reasonable understanding of their risks. However, the NRA and SNRAs are high-level policy documents that inform this understanding and do not provide sufficient granularity on specific sectoral risks. Some high-risk areas, including NPOs and legal persons and arrangements, lack a detailed risk assessment to

improve risk understanding and inform policy and operational responses.

7. The key strength of the Dutch system lies on its robust domestic co-ordination and co-operation on AML/CFT issues at both the policy and operational levels. The Netherlands demonstrated significant AML/CFT co-operation and collaboration at the public-public, public-private and private-private levels.
8. National AML/CFT policies largely address identified ML/TF risks. For instance, the ML Action Plan is targeting the ML risks identified in the ML NRA and the SNRA. The risk assessment process is defined as an on-going process, resulting in amendments to policies to mitigate new or emerging ML/TF risks. However, a number of AML/CFT exemptions exist in the BES Islands, which are inconsistent with the risk assessments.
9. Some FIs, DNFBPs and NPOs were directly involved in the development of the NRAs. The results of risk assessments were also communicated to obliged entities in a proactive and consistent manner.

Recommended Actions

1. The Netherlands should continue its persistent efforts to improving the quality and utility of ML/TF NRAs by:
    - expanding the scope to cover the ML threats associated with the underlying predicate offences, including the origins of proceeds, rather than focusing solely on the ML methods and channels;
    - expanding the categorisation of the risks of different FI and DNFBP sectors compared to each other at the national level using the same assessment standard; and
    - validating qualitative inputs with quantitative data, including prosecution data, LEA investigations, STR information and international requests/spontaneous co-operation in more recent years.
2. The Netherlands should develop a more detailed risk assessment for legal persons and arrangements and the NPO sector. Such assessments should include engagement with relevant private sector entities, including NPOs representing different parts of the sector.
3. The Netherlands should continue efforts to conduct more targeted and proactive measures against high risk areas, in particular against underground banking activity which is identified in both ML and TF NRAs.
4. The Netherlands should remove its exemptions for DNFBPs in the BES Islands related to identifying and assessing ML/TF risks and having policies to mitigate risks.

85. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.

Immediate Outcome 1 (Risk, Policy and Co-ordination)

86. The Netherlands has a good understanding of its ML/TF risks, which is primarily informed by a continuous risk assessment process. The Assessment Team based this conclusion on a review of the NRAs and interviews with authorities and private sector representatives (including representatives from the non-profit sector).

87. The Netherlands has issued a total of six NRAs: two ML NRAs (in 2017 and 2020); two TF NRAs (in 2017 and 2020); and two ML/TF NRA for the BES Islands (in 2018 and 2021). All NRAs were developed by the WODC (the Research and Documentation Centre) of the Ministry of Justice and Security. The methodology was based on a previous study conducted by the WODC, which concluded that the ISO 31000 risk management framework is most suitable for this purpose. In short, this research methodology involves:

- A literature review of key characteristics of the Netherlands that influence the prevalence of ML/TF (e.g., socio-cultural, economic, geographical and criminal factors);
- A survey circulated to authorities and experts to indicate the prevalence of ML/TF threats, methods and channels;
- Expert meetings with policy, supervisory, law enforcement and private sector authorities to identify ML/TF threats with the greatest potential impact;
- Multiple interviews with experts, including to assess and validate the resilience of the available policy instruments to prevent ML/TF; and
- Quantitative data (e.g., a study of criminal proceeds) for the description of the risk context and – to a limited extent to analyse ML/TF risks.

88. In accordance with this methodology, the NRAs identify, analyse and categorise the ML/TF risks having the greatest potential impact, as well as the resilience of policy instruments (laws, regulations, etc.) aimed at prevention and mitigation of ML/TF. The NRAs do not include a breakdown of threats based on predicate offences, but instead outline the risks associated with various methods and channels. Information related to the general criminal situation, including statistics, was included in the background contextual analysis of the NRAs. This methodological approach is justified by authorities as LEAs are required to pursue ML cases regardless of the underlying predicate offence. That considered, a better understanding of the ML risks associated with underlying predicate offences, may be valuable to inform risk-based policies, strategies, measures and resource allocation.

89. The NRAs are largely driven by qualitative data, including expert judgements from the participating experts and independent reports such as the EC's SNRA and EUROPOL's Internet Organised Crime Threat Assessment. Given the materiality of expert judgements, the methodology was refined in the second NRA to increase the amount of experts consulted and the number of meetings and interviews held in order to deepen the understanding of ML/TF risks.

90. Quantitative input included an overview of reported crimes (e.g., on property crime, theft and fraud) and a study of criminal proceeds (e.g., fraud and drug crimes), the latter of which includes data from up to 18 years ago. While the WODC attempted to carry out more comprehensive quantitative analysis to supplement the NRAs, it was unsuccessful due to issues related to data privacy and obtaining timely consent. The WODC is aware of these statistical deficiencies and is examining ways it can enrich its analysis with more quantitative data for the next NRAs. For example, the WODC aims to include conviction and enforcement data in the preparation of the upcoming NRAs.

91. The NRAs were drafted in a coordinated manner, with all relevant authorities participating in various stages of the process (e.g., as experts and/or survey respondents). The private sector was also engaged as experts.

92. The ML risks identified by authorities are reasonable, consistent and in line with international feedback received from FATF and FSRB delegations. Fraud and drug-related offences are identified as the most significant predicate offences contributing to the highest ML threats, based on the separate study commissioned by the WODC in 2018 on the nature and scope of criminal expenditure between 2004 and 2014. The authorities state that the associated criminal proceeds of these offences both transit through and remain in the Netherlands. The highest ML risks, when taking into account various policy instruments and other mitigation measures, are ML through: the use of virtual assets; trade-based services; underground banking, including unlicensed payment services; offshore companies; and services/goods of dealers of high-value goods. The ML NRAs do not categorise the risk levels of FI and DNFBP sectors at national level using the same assessment standard, which may assist with risk mitigation and resource allocation. Instead, the ML NRAs identified the ML methods/channels of higher risk, including banks, trust offices, VASPs, unlicensed/licensed payment institutions (including MVTS) and dealers in high value goods.

93. The TF risks identified by the Dutch authorities are informed by the TF NRAs and terrorism threat assessments and are comprehensive and in line with international feedback. The Dutch authorities consistently demonstrated a shared understanding of the Netherlands' TF risks in line with the TF NRAs. Terrorism related to religious extremism presents the main TF risk, but other terrorism threats exist, including right-wing terrorism. The highest TF risks come from the acquisition of funds and the financing of terrorism through NPOs both in the Netherlands and abroad, TF with the personal means of the financier, as well as the moving of funds through underground banking including unlicensed payment services. These risks align with the TF cases submitted, including a large percentage of cases in which funds were provided to family members to participate in terrorist organisations in conflict zones.

94. In addition to the NRAs, the Netherlands' risk understanding is also based on sectoral risk assessments that guide risk-based supervisory activities. For example, in 2020 a detailed sector assessment was published on the casino/gaming sector. However, the Dutch authorities have not undertaken a more detailed sectoral assessment of risks associated with the types of legal persons and legal arrangements and the NPO sector. Given the materiality and the risks present, the Netherlands should conduct a thorough assessment of the ML/TF threats and vulnerabilities of such high risk areas in order to consider possible additional risk-based measures.

95. In addition, a number of thematic studies have been conducted through various platforms with the joint efforts of policy, supervisory, law enforcement and private sector authorities to identify emerging ML/TF risks for policy and operational purposes. For instance, FIU-NL (in collaboration with the Police, OM and AMLC) has conducted studies into underground banking and virtual assets in 2016 and 2017, respectively. Both studies resulted in typologies, which are publicly available on the website of FIU-NL.

96. Many of the FIs and firms met by the Assessment Team were aware of the ML and TF NRAs' conclusions but noted that the NRAs and SNRAs are high-level policy documents that do not provide sufficient granularity on their specific sectoral risks.

97. For the BES Islands, the authorities have a less informed but adequate understanding of the islands' ML/TF risks as outlined in the BES NRAs. This understanding is predominately informed by expert judgements and FIU-NL data. The WODC experienced significant difficulties in obtaining basic quantitative data to inform the BES NRAs. For example, the BES Police (KPCN) is unable to provide the number of drug-related offences and arrests after 2017. However, there were improvements in accessing relevant statistics in the recent 2021 NRA. Moreover, the lack of local knowledge about financial crime amongst LEAs and the reluctance of the local community to report crimes, as addressed in the NRA, might have resulted in an information gap in the understanding of ML/TF risks. According to the NRA, the highest ML risk lies in the real estate sector, in particular large cash transactions. The NRAs briefly touch upon TF, but do not include a detailed assessment, as there were no authorities who were aware of any indication of terrorism or TF in the BES Islands. All competent authorities consistently reiterated this conclusion during interviews with the Assessment Team.

National policies to address identified ML/TF risks

98. In general, national AML/CFT policies appropriately address identified ML/TF risks. The Assessment Team based this conclusion on a review of available AML/CFT Action Plan and Statements and various policy instruments and discussions with authorities and private sector representatives.

99. A key strength of the Dutch system is the close domestic co-ordination and co-operation, including for ML/TF risk assessment and the development of risk-based strategies/policies. This collaboration occurs through established working groups at the public-public and public-private levels (see Table 1.1 in Chapter 1). This institutional co-operation facilitates information sharing when conducting risk assessments, pursuing project-based investigations and developing national policies aimed at addressing identified ML/TF risks.

100. The Netherlands developed its national AML/CFT policies based on the findings of the various NRAs and other risk-based initiatives, such as thematic studies and sector risk assessments. For instance, following the ML NRA 2017, the Minister of Finance and the Minister of Justice and Security jointly formulated an AML policy in 2019, entitled the ML Action Plan. This Action Plan is a national-wide and comprehensive policy targeting the ML risks identified in the ML NRA and the SNRA.

101. The ML Action Plan clearly outlines national AML/CFT measures around three pillars: (1) raising barriers; (2) increasing the effectiveness of the gatekeeper function and supervision; and (3) strengthening investigation and prosecution. The pillars include measures such as enhancing transparency of legal persons and arrangements, a prohibition on cash transactions over EUR 3 000 for dealers in goods, regulation of VAs, strengthening the AML/CFT framework in the BES Islands; increasing supervisory and LEA resources. This Action Plan is also supported by thematic projects (e.g., by FEC, AMLC and FIU-NL), the Strategic Program AML and by a series of programmes, such as a national programme targeting organised, subversive crime and initiatives on the confiscation of criminal assets. All of these measures are intended to mitigate the residual risks identified in the ML NRAs.

102. The ML Action Plan and its progress reports were presented by the Minister of Finance and the Minister of Justice and Security to the Parliament, which is a clear indication of the high-level commitment afforded to it by the Dutch authorities. These policy responses are reviewed and updated as part of a policy cycle, which is repeated bi-annually to ensure that the risk assessment and policies in the area of AML/CFT remain up-to-date. Most of the Action Plan items have been completed while the remaining actions are reported to be on track.

103. The National Coordinator for Security and Counterterrorism, under the Ministry of Justice and Security, is responsible for counter-terrorism (CT) policy and strategy. The national CT policy is outlined in the National Counterterrorism Strategy 2016-2020, which involves all government partners in the fight against terrorism. CFT is a core component of the CT policy, and embedded in the intervention areas of procuring, preventing and pursuing.

104. In September 2020, the Minister of Finance and the Minister of Justice and Security issued a TF Policy Statement to Parliament in response to the 2019 TF NRA. This Statement refers to existing measures taken to mitigate risks related to TF via foundations or other legal forms, to TF using underground and hawala banking, and the movement of cash and TF via VAs.

105. Similar to the ML Action Plan, a number of additional measures have been implemented to mitigate TF risks. For example, additional resources are allocated to the Police and FIOD for TF investigation, the Terrorist Financing Programme within the FEC is running a sub-project to map the foreign financing of NPOs that could be related to TF, and the FIU-NL has developed TF risk profiles to increase the knowledge and understanding of obliged entities.

106. For the BES Islands, the ML Action Plan seeks to address identified ML/TF risks by strengthening AML/CFT legislation and enhancing the knowledge and capacity of local authorities. No CFT policies or strategies are in place for the BES Islands, which aligns with its risk profile based on the limited qualitative and quantitative information available.

107. In general, the national policies and strategies in place are in line with the Netherlands ML and TF risks.

Exemptions, enhanced and simplified measures

108. The Netherlands legal framework for exemptions and applying enhanced measures are largely related to the EU's Anti-Money Laundering Directives. For example, certain issuers of electronic money (i.e., prepaid cards that can be exchanged with multiple parties) are exempted from the obligation to conduct CDD under a number of strict conditions, such as low amounts and restriction to spend in the Netherlands. This exemption is based on the EU's AMLD5 and the low risks identified in the SNRA and NRA.

109. For the BES Islands, DNFBPs (except for trust offices) are exempt from the following obligations:

- Identifying and assessing its ML and TF risks;
- Having in place policies, procedures and measures to mitigate ML and TF risks identified in the NRA;
- Designate a person to be responsible for ensuring compliance with the AML/CFT obligations in the Wwft BES; and
- Implementing group-wide policies and procedures.

110. These exemptions are not in line with the ML risks identified in the updated BES NRAs of 2021, as the purchase of real estate and the use of legal entities is identified as carrying ML risks.

111. In the Netherlands, only one casino (with multiple branches) is licensed and regulated under the AML/CFT legislation. Other stakeholders in the physical gaming sector such as providers of lotteries, slot machines, horse racing and sports betting are exempted from AML/CFT requirements. These exemptions are based on the sectoral ML/TF risk assessments commissioned by the WODC in 2017 and 2020. Online gambling is subject to a licensing regime and the AML/CFT requirements extend to the aforementioned exempted gaming sectors.

112. Valuers of real estate and dealers in vehicles, vessels, antiques and art are supervised for AML/CFT due to EU requirements and identified ML/TF risks. In the BES Islands, dealers in construction materials are also included in AML/CFT legislation. While these AML/CFT requirements (beyond real estate and DPMS) are not part of the FATF Standards, the inclusion of these high-value sectors demonstrates that the Netherlands is proactively including sectors it identifies as high risk in the NRAs. The Assessment Team did not meet representatives or assess the level of AML/CFT effectiveness in the sectors that are not covered by the FATF Standards.

Objectives and activities of competent authorities

113. The risk assessments have informed the objectives and activities of authorities. At the policy level, the authorities have introduced a number of legislative amendments to address ML/TF risks. Some of these legislative amendments respond to ML/TF risks identified in the European SNRA, and are elements required by EU AML Directives. Recent amendments include the introduction of:

- a public BO register for legal persons;
- Customs supervision and enforcement with respect to the transport of currency and other liquid assets within the EU;

- regulation of VASPs;
- a separate AML/CFT legislation on trust offices;
- AML/CFT regulation for online gambling; and
- amendments in the BES Islands for obliged entities in order to strengthen AML/CFT compliance.

114. At the operational level, the OM in consultation with the FIU-NL, FIOD and Police, has established the Strategic Program AML 2019-2022, which aims to enhance coherence and synergy amongst parties to better align their activities with the ML risks identified in the ML NRA 2017. The programme sets out specific thematic priorities, such as concealed assets and trade-based money laundering (TBML). In addition, specific strategies have been formulated to mitigate the major ML threats in the Netherlands, including organised, subversive crime with a focus on drug-related crimes and separate strategies on fraud. The below case study box summarises a recent initiative to combat organised, subversive crime and obstruct the criminal revenue model.

Box 2.1. Multidisciplinary Intervention Team

The Multidisciplinary Intervention Team (MIT)[33], established in 2020, focuses on organised, subversive criminality. The objective of the MIT is to dismantle the dominant positions of criminal leaders and their facilitators, and put up barriers against the misuse of the legal economy and infrastructure through criminal law as well as surveillance, enforcement, administrative law and taxation.

The MIT was set up at the initiative of the Ministry of Justice and Security. Specialists in the area of intelligence, digital, international and financial investigations from various units cooperate in the MIT (OM, Police, FIOD, KMar/Defence, Customs, and the Tax and Customs Administration). A specific area of focus of the MIT is the confiscation of criminal proceeds.

The purpose of the MIT is to establish an overview of the activities related to organised, subversive criminality. The establishment of this team, which in part covers ML, was in response to the country's assessment of risks, particularly risks related to organised criminal activity and drug trafficking.

115. The Dutch authorities have a robust CFT framework to address TF risks, for instance through the FEC TF Programme and FEC TFTF, which identify TF signals for corresponding preventive, supervisory and enforcement activities. There is also an integrated approach to CT and jihadism, which includes co-operation amongst national and regional LEAs and FIU-NL. These measures seek to prevent and repress extremism and terrorism, including TF. The key objectives of the approach are the strengthening of information exchange and the early identification of and response to the threats posed by radicalised persons.

33 As of 1 July 2022, the MIT changed its name to 'National Collaboration against Organised Crime' (NSOC) and has specified its operational focus on Trade Based Money Laundering, the criminal abuse of financial service providers and logistic services, and fighting corruption and violence.

116. The FIU-NL also organises its analytical priorities based on system queries informed by ML/TF risks. This ensures that the FIU's analytical and strategic products respond to the country's priorities and ML/TF risks (see IO.6 for more information). FIU-NL has also completed other risk-based studies resulting in refined indicators circulated to obliged entities to better detect these high-risk activities. For example in 2016, FIU-NL completed a study on underground banking and established new indicators/typologies for obliged entities, and in 2019 the FIU-NL circulated indicators to identify high-risk NPOs.

117. At the AML/CFT supervisory level, supervisors, in particular DNB and AFM, are committed to the implementation of measures under the national AML/CFT policies. AML/CFT supervisors conduct additional sectoral assessments, trend analyses and good practice studies to intensify their understanding of the sectoral ML/TF risks. For example, DNB issued two good practices documents on bank and trust office customer tax integrity risk in 2019; and AFM conducted a thematic investigation on investment institutions on VAs.

National co-ordination and co-operation

118. The key strength of the Dutch system lies its robust domestic co-ordination and co-operation on AML/CFT issues at both the policy and operational levels. The Netherlands leverages a number of platforms to facilitate public-public and public-private partnerships to coordinate on AML/CFT and CPF. As noted in Chapter 1 (see table 1.1), there are extensive co-ordination bodies focusing on policy and operational matters, including bodies on thematic priorities.

119. At the policy level, this co-ordination is largely led by the Ministry of Justice and Security and the Ministry of Finance, which report to Parliament every six months on progress against the ML Action Plan. The Ministers of Finance, Justice and Security, and Foreign Affairs are jointly responsible for CFT and CPF policy.

120. At the operation level, there are a large number of formal and informal co-ordination bodies. These bodies (1) implement measures taken on a national level, for example in the 2019 ML Action Plan, (2) address risks assessed at a national level with specific projects and, (3) perform exploratory or additional research into specific risks. The main co-ordination bodies for AML/CFT on operational and/or supervisory issues are:

- **FEC**, established in 1998, is responsible for protecting and strengthening the integrity of the financial sector. The FEC exchanges strategic and tactical information, shares knowledge and expertise, and conducts projects, a structural Programme on CFT and two Taskforces (TF Task Force and Serious Crime Task Force), including private sector partners. Primary participants include AFM; DNB; FIOD; FIU-NL; Police; OM and the Tax and Customs Administration.

- **AMLC**, established in 2013 by the FIOD, contributes to the formulation of new ML typologies for use in criminal investigations, facilitates to launch major NL investigations, draws up specific phenomenon descriptions, runs projects, builds and manages unique data availability, supported by a wide-ranging intelligence position. Primary participants include FIOD, Police, FIU-NL, OM, KMar, Tax and Customs Administration and private sector partners.

- **RIECs**, established in 2008, enhance awareness and support administrative authorities with combatting organised crime, support regional co-operation by exchanging strategic and tactical information, providing expertise and information, intelligence, and reinforce resilience on the regional/local level. Participants include: FIOD; Police; Municipal/Provincial authorities; KMar, OM, Tax and Customs Administration etc.

- **Consultation Team on Non-Reporting Obliged Entities**, established in 2012, is a selection committee chaired by the OM. During the consultations, supervisors and the FIU-NL present matters that may qualify for criminal investigation into breaches of the Wwft or other compliance legislation, such as the Wtt, by obliged entities, which are punishable in the Economic Offences Act.
- **Obliged Entities Committee**, established in 2008, discuss (proposed) legislation and policy plans that relate to the organisation and performance of the obligation to report UTRs and the objective indicators for establishing whether a transaction is unusual. Participants include obliged entities and public authorities.
- Important **operational co-operation** also includes sharing and combining of data institutionalised in co-operation mechanisms like iCOV, AMLC Suite, JustisTRACK and CT Infobox (See also IO.6).

121. In addition to public-public and public-private coordinating bodies, the Netherlands also has a number of private-private initiatives on AML/CFT. The below case study box outlines a recent initiative of the private sector to provide new insights into potential ML/TF across the Dutch banking sector.

Box 2.2. Transaction Monitoring Netherlands (TMNL)

Launched in 2020, TMNL is a joint initiative of five Dutch banks to collectively monitor their transactions to identify signals that could indicate ML/TF. Through collective transaction monitoring of combined transaction data, the primary goal of this initiative is to improve the detection of ML/TF by identifying unusual transaction patterns that individual banks cannot identify alone. As such, TMNL will focus on so-called multi-bank alerts. The privacy sensitive information of the transaction data to be exchanged between the banks and TMNL is pseudonymised. Currently, the utility is solely focusing on transaction information related to corporate clients.

122. For CPF activities and PF TFS, various coordinating bodies exist, focusing on the implementation of sanctions in general (the *Sw* Consultation Meeting and the Inter-ministerial Sanctions Consultation Meeting), on taking specific freezing measures (Asset Freezing Committee), and on consulting with banks and insurers on implementing TFS (Sanctions Experts Pool). Representatives of DNB, AFM and of the OM are present during these consultations. In addition, the co-operation between the OM, the Ministry of Foreign Affairs, Customs, and FIOD in the field of export controls for dual-use goods and the Carré Consultations increase knowledge on PF sanctions evasion. Such co-operation also helps ensure that any signals of PF are disseminated to and actioned by the relevant authority (e.g., supervisor, intelligence service, or LEAs).

Private sector's awareness of risks

123. The Netherlands has undertaken extensive outreach to ensure that the private sector was involved in the development of the NRAs, and received the final version of the assessments via dissemination by competent authorities. All NRAs, including the SNRAs, are also available on publicly accessible webpages, in English and Dutch. FIs, DNFBPs and other sectors met by the Assessment Team are aware of the relevant results of the ML/TF NRAs. This is in line with the legal obligations as obliged entities are required to take into account the NRAs when adopting risk mitigating policies, procedures and measures.

124. The below private sector entities were involved in the development of the NRAs. These entities acted as experts and survey respondents:

- Major banks (all as survey respondents and experts in in-depth interviews, while one bank was also included in the expert meetings and validating interviews)
- Umbrella NPO organisation (as a survey respondent)
- DNFBPs (all as survey respondents, while some in interviews and meetings)
- BES Islands obliged entities as experts to identify potential ML threats.

125. In terms of proactive circulation of the NRA results to FIs and DNFBPs, the NRAs were also included in the agendas of meetings of the Obliged Entities Committee. Supervisors also disseminated the findings of NRAs to their respective sectors, and integrated the findings into sector guidance (e.g., the DNB guidance on Wwft and Sw, and Wwft guidance for lawyers of the NOvA). The AMLC also incorporated the NRAs into training materials for obliged entities and competent authorities.

126. Regarding the TF risk understanding of the NPO sector, the Netherlands has a strong collaborative approach with self-registered NPOs (i.e., so-called "good faith" NPOs). The NPO sector was informed of the NRAs through meetings held by the Ministry of Justice and Security, the Ministry of Finance, and the Ministry of Foreign Affairs, as well as through fact sheets prepared in consultation with and disseminated to the sector. The representatives of the NPO sector met by the Assessment Team had a strong understanding of the TF vulnerabilities. These representatives also expressed the need for a more detailed NPO risk assessment, as the findings of the NRAs are regarded as high-level policy documents. Moreover, the sector emphasised the need for more engagement and with a broader range of NPO participants in the next assessment of the TF risks in the NPO sector. The Assessment Team concurs with this view, as a more detailed sectoral assessment with enhanced engagement will provide a more comprehensive overview of the threats and vulnerabilities of the NPO sector, which could also consider the self-regulatory measures already in place in the sector.

2

Overall Conclusion on IO.1

1. Overall, the Netherlands has a good understanding of its ML/TF risks, with a relatively stronger understanding on TF. ML and TF risks identified seem reasonable and in line with feedback received from FATF/FSRB members. National AML/CFT policies, strategies and activities are formulated and implemented in a targeted manner to address identified ML/TF risks, though some exemptions are inconsistent with the BES Islands' risk profile. The objectives and activities of the competent authorities seek to address or mitigate identified risks.
2. The key strength of the Dutch system lies its robust domestic co-ordination and co-operation on AML/CFT issues at both the policy and operational levels. The Netherlands also leverages a number of platforms to facilitate different forms of partnerships (public-public, public-private and private-private) to coordinate on AML/CFT as well as public-public platforms on CPF.
3. There is room for improving ML/TF risk understanding by including more relevant information in the NRAs and providing sufficient granularity on specific sectoral risks.
4. The Netherlands is rated as having a substantial level of effectiveness for IO.1.

Chapter 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Immediate Outcome 6

1. LEAs have access to a broad range of financial intelligence and information to conduct their investigations into ML, TF and predicate offences and to trace criminal proceeds. Datahubs, in particular iCOV and AMLC Suite, are a strong feature of the Dutch model of financial intelligence, as they provide LEAs with FIU disseminations and a wide spectrum of other information in a timely manner to fit investigative needs. Investigators regularly use these data sources to enrich their analysis and identify criminal assets or criminal connections.
2. The FIU-NL plays a central role in the production and dissemination of financial intelligence. It has improved its analytical capacities to process a considerable and increasing amount of information included in its UTR database, by investing in system queries and automation. FIU-NL uploads its disseminations on Blueview, which is directly accessible by LEAs, as well as in iCOV and AMLC Suite.
3. FIU-NL's analytical products—both in relation to operational and strategic analysis—are of high quality and targeted to identified ML/TF risks and operational needs of LEAs. In recent years, approximately 60% of FIOD investigations have direct linkages to the FIU-NL disseminations, and half of all TF investigations are triggered by FIU-NL's analytical products. FIU-NL also performs strategic analysis, including new ML typologies, in general in co-operation with AMLC and the OM.
4. Inter-agency co-operation platforms, including Programme FEC TF, public-private partnerships, such as the FEC TF Task Force and Serious Crime Task Force and the Fintell Alliance, and the long-established operational synergy between LEAs and FIU-NL, are additional strengths of the Dutch system to gather financial evidence, share best practices and discuss operational activities.
5. There are some minor concerns in relation to the unavailability of data on the extent of FIU disseminations left unattended in Blueview, and of the usage of FIU's disseminations in police investigations into ML and predicate offences. These are largely mitigated by the extensive co-operation between LEAs and the FIU-NL, and the frequent use of datahubs by the police.

Immediate Outcome 7

1. The Netherlands proactively initiates ML investigations, through police intelligence signals detected in the course of investigations into predicate offences, as well as through financial intelligence developed by the FIU-NL. In addition, the authorities adopted an innovative approach by launching thematic AML projects based on the ML risks in the NRAs to increase their ability to detect new ML schemes and typologies, resulting in additional cases identified. Queries

in the iCOV, AMLC and JustisTRACK datahubs enable investigators to gain financial insights into suspects and their networks.

2. The high level of expertise, and extensive co-operation between all competent authorities involved in ML investigations are strengths of the Dutch investigative system. LEAs use a wide range of special investigation techniques to access documents and information. However, there are persisting challenges in accessing the information protected by legal professional privilege in a timely manner.

3. A national AML Prosecutor ensures co-ordination at policy and operational levels. The Steering Team coordinates and prioritises most complex ML investigations at national level and has initiated over 700 investigations since 2016. ML investigations are generally aligned with the country's ML risks. As no comprehensive statistics on underlying predicate offences or types of ML are maintained, this conclusion is based on the consideration of the large number of cases studies provided by the authorities. Similarly, the authorities demonstrated their ability to investigate and prosecute different types of ML, including stand-alone, third party ML and ML investigations into foreign predicate offences. Since 2016, the Netherlands has pursued more than 17 000 ML investigations at regional and national levels. Investigations at regional level cover all types of ML, but are generally less complex, with a majority of self-laundering cases.

4. The OM has wide discretionary powers in deciding whether to prosecute a case for ML. There is a relatively high number of cases dismissed, or concluded through out of court settlements. This is not limited to situations where it is not possible to secure a ML conviction, but it also due to the priority given to confiscation efforts, and to the overall length of trials.

5. The Netherlands has a good conviction rate of ML cases which are brought to court (62% of final convictions in the first instance). Sanctions applied to ML cases are low, thereby limiting their dissuasiveness and effectiveness. The lack of ML sentencing guidelines for judges, and the breaches of the principle of undue delays impact on final ML sentences.

6. In the BES Islands, the establishment of a specialised ML prosecutor, additional financial training and close co-operation between KPCN and RST are important steps to streamline the authorities' approach to ML cases. LEAs are mainly relying on support from continental Netherlands as well as police staff in the Kingdom to handle complex financial investigations. The lack of stand-alone ML investigations and the limited number of cases where the OM BES pursued a ML charge are indicative of an investigative approach mainly focused on predicate offences.

Immediate Outcome 8

1. The Netherlands pursues confiscation as a policy and strategic objective. At an operational level, there is a clear instruction to LEAs to pursue a financial investigation in parallel to criminal investigations. Additional resources are allocated to LEAs and OM to strengthen capacities to trace and confiscate assets, including in complex cases involving VAs, and to improve co-ordination, through a National Confiscation Steering Team. There are effective mechanisms in place to register, manage and store seized and confiscated goods.

2. The Netherlands has a comprehensive regime to deprive criminals of their assets, through object and value confiscations. The OM retains discretion in deciding

whether to pursue confiscation through a court proceeding or an out of court settlement. The Dutch approach on reversal of the burden of proof on the convicted person to demonstrate the licit origin of income or assets, in case of a conviction for serious and lucrative crime, is a particular strength of the confiscation system. Tax and administrative measures are used to complement the criminal approach.

3. The statistics available on seizures and confiscations offer a partial image of the results achieved by the authorities in depriving criminals of their proceeds, and providing restitution to victims. However, they demonstrate a correlation between seizure results and the prevailing proceeds generating offences. The Netherlands demonstrated strong and effective co-operation with international counterparts to trace and seize criminal assets.

4. Customs have extensive investigative powers to perform their tasks, and seize cash or valuable goods whenever there is a false declaration. The very low threshold to initiate a ML investigation resulted in a good number of seizures and ML cases transmitted to LEAs. The sanctions applied to violations of the obligation to declare in both the Netherlands and the BES Islands are low, which limits their dissuasiveness.

5. In the BES Islands, there have been 12 confiscation cases between 2017 and 2020. While the annual confiscation target was achieved in terms of value of confiscated proceeds, in the absence of more detailed information the Assessment Team cannot establish whether these results are consistent with the risks. Furthermore, the limited expertise noted in IO.7 in relation to the conduct of financial investigation in the BES Islands may also impact the ability of the authorities to pursue confiscation.

Recommended Actions

Immediate Outcome 6

1. The Netherlands should develop a systematic feedback mechanism to provide information to the FIU-NL on the follow-up given by LEAs to the disseminations in Blueview, and to identify the disseminations left unattended.
2. The Netherlands should systematically track the extent of the use of FIU's disseminations and other financial intelligence reports in ML, TF and predicate offence investigations, prosecutions and convictions.
3. The FIU-NL should continue its efforts to ensure that its products are timely and of high quality, given the increasing number of UTRs submitted and increasing demands from various co-ordination and co-operation platforms.

Immediate Outcome 7

1. The Netherlands should collect comprehensive statistics on ML investigations, prosecutions and convictions, including on the underlying predicate offences in

mixed cases, and on the types of ML offences investigated. The statistics should inform future ML NRA updates.

2. The Netherlands should review the ML sentencing regime to ensure that penalties applied are sufficiently dissuasive and develop specific ML orientation points (i.e., akin to sentencing guidelines), which include factors to consider when determining the penalty based on the gravity of the offence.
3. The OM should ensure that a higher and more gradual range of penalties is demanded in practice.
4. The Netherlands should enhance its efforts to reduce the delays in deciding the cases where the legal professional privilege has been invoked in Courts, by streamlining the judicial procedures to filter and assess these requests.
5. The Netherlands should review the resources allocated to the judges and prosecutors to ensure that ML investigations are timely, of high quality and with a minimum of undue delay.

BES Islands

6. KPCN should strengthen the training of its police force, to increase their ability to investigate ML. The Netherlands should continue assisting and providing additional expertise to KPCN.
7. BES LEAs should prioritise the investigation and prosecution of ML cases, in line with the risks and should pursue stand-alone ML investigations.
8. BES authorities should review the level of sentencing applied in practice to ML cases, and consider the development of sentencing guidelines or points of reference to guide the OM and judges.

Immediate Outcome 8

1. The authorities should improve the collection of comprehensive and reliable statistics on seizure and confiscation to measure the success of their confiscation policies.
2. The Netherlands should enhance its efforts to recover criminal proceeds located abroad and collect more extensive statistical data in this respect.
3. The Netherlands, including BES Islands, should review the maximum level of fines applicable for failure to declare cash/BNI, to ensure that the penalties are proportionate to the amount involved, and dissuasive.
4. LEAs and OM BES should review their annual confiscation target, taking as a baseline the results achieved in recent years.

127. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

128. LEAs, in particular FIOD and the Police, routinely use financial intelligence in their investigations into ML, TF and predicate offences to develop evidence and trace criminal proceeds. As the conduct of parallel financial investigations is a common practice across all LEAs, various financial investigation teams directly access and process financial information. The FIU-NL plays an important role in the production of financial intelligence products for ML, TF and predicate offence investigations.

129. As noted in the TC Annex, FIU-NL is the national centre for the receipt and analysis of suspicious transaction reports and threshold reports submitted by obliged entities in continental Netherlands and the BES Islands. The Netherlands refers to both suspicious transaction reports and threshold reports (e.g., on cash payments over EUR 3 000) jointly as "unusual transaction reports" (UTRs). Obliged entities must submit UTRs to the FIU through goAML on the basis of a subjective indicator (i.e., reason to believe that a transaction may be related to ML/TF) or objective indicators (i.e., threshold reports), which significantly enrich the FIU-NL data pool (see table 3.5). UTRs are available only to the FIU-NL and not accessible to LEAs. When the FIU produces a dissemination report[34] based on its analysis, data matching, or requests (see further details in the section below) and uploads it in various databases, LEAs have access to it. An overview of the number of UTRs received by the FIU-NL, and on the number of disseminations is included in Table 3.1 below.

Table 3.1. FIU analysis: number of UTRs and disseminations

	2016	2017	2018	2019	2020	2021*
Total UTRs received [subjective *vs* objective indicators]	417 067	361 015 [68%;32%]	39 4743 [69%;31%]	54 1236 [59%;41%]	722 247 [57%;43%]	1 098 913 [44%;56%]
FIU disseminations (% of UTRs disseminated)	53 533 (12.8%)	40 546 (11.2%)	57 950 (14.7%)	39 544 (7.3%)	10 3947 (14.4%)	80 448 (7.3%)
Split based on reason for FIU-NL dissemination						
Match with VROS/CJIB databases	29 266	18 502	32 488	12 104	42 440	35 859
FIU-NL own investigation**	16 555	14 875	17 982	18 963	54 884	37 991
Of which, number initiated by foreign requests	*(900)*	*(976)*	*(1 139)*	*(2 999)*	*(4 015)*	*(6 452)*
LEAs (LOvJ) requests	7 712	7 169	7 480	8 477	6 623	6598

* Covers the period up to 18 November.
**These figures include FIU-NL analysis based on foreign requests.
Note: The table includes UTRs and disseminations in both continental Netherlands and the BES Islands.

[34] The Netherlands refers to its FIU disseminations to LEAs as suspicious transaction reports (STRs). As the term STRs is defined differently by the FATF Standards and globally used to refer to the information reported to the FIU from reporting entities, the Assessment Team instead uses the word "dissemination" to avoid confusion.

130. Since 2019, the number of UTRs has increased significantly. This is partly due to an increase in reports filed by banks following a significant financial penalty imposed on two major Dutch banks for non-compliance with AML/CFT requirements (see IO.4 for the breakdown of UTRs filed over the assessment period). Furthermore, this increase is also due to specific FIU alerts related to COVID-19 related fraud (see Box 3.3), and to the regulation of VASPs, which became obliged entities in 2020 and are subject to reporting obligations since May 2021. The decrease of disseminations in 2019 is caused by a temporary suspension of the cross-matching of UTRs with the Criminal Records database (VROS) between October 2019 and September 2020, due to technical issues. A significant increase in the disseminations based on the VROS matching and FIU own investigations was noted in 2020 and 2021. This is due to several factors, including the resumption of the VROS matching, and of the FIU work to refine its automation system to improve UTR analysis.

131. The FIU-NL also receives UTRs from the BES Islands, and makes disseminations to LEAs in the BES Islands (see Table 3.2). In performing investigations on the BES, FIU-NL has access to additional sources of information, including the RST list of suspects in ongoing investigations. FIU-NL and BES LEAs can also consult the BES land registry, BES CoC and other registries and information to gain financial insights into suspects. FIU-NL also shares pseudonymised information with the other FIUs of the Kingdom through FCI.net (see IO.2).

Table 3.2. UTRs and disseminations in the BES Islands

	2016	2017	2018	2019	2020	2021*
Total UTRs received	1 038	1 037	993	1 031	858	1 681
Disseminations to LEAs (%)	231 (22%)	337 (32%)	174 (18%)	276 (27%)	107 (12%)	114 (7%)

* Covers the period up to 18 November.

132. The FIU-NL provides quarterly reports to sectoral supervisors with a breakdown of UTRs filed by individual FIs and DNFBPs. These reports include aggregated information per individual obliged entity on their reporting behaviours (e.g., transaction date, reporting date, total of UTRs and disseminations, the indicators and length of the transaction description). Acting on specific requests by supervisors, the FIU-NL supplements this with additional information such as reporting behaviours, which allow supervisors to take a risk-based approach in performing their statutory duties. The number of such requests has increased over recent years, reflecting a more targeted and risk-based approach to AML/CFT supervision, and a recognition of the importance of the FIU-NL's information.

133. During criminal investigations, LEAs have direct access to FIU's disseminations via Blueview and systematically use financial and tax information and network analysis obtained by submitting requests to different financial intelligence datahubs (see Box 3.1 below). Through these datahubs, LEAs can proactively gather a holistic financial overview in a timely manner, without the need to consult each data source separately. This is a key strength of the Dutch system on the access and use of financial intelligence.

Box 3.1. Non-exhaustive list of financial intelligence datahubs

Criminal and Unexplained Assets Infobox (iCOV): is a partnership of 13 authorities, including LEAs, OM, and FIU-NL, which provides and develops data-driven intelligence reports. Over 22 datasets (e.g., FIU disseminations, land register, CoC register, and tax information) are linked to track criminal and unexplained assets, to uncover ML and fraud. iCOV reports are generated within a few minutes to a few hours. There are three types of reports: assets and income reports (financial situation of a specific subject), relation reports (financial and business relations of a natural or legal person) and thematic reports (insights into ML through real estate or another specific theme). iCOV reports are used by more than 4 200 authorised users, whereby each user has insight into the specific information for which they are legally permitted.

AMLC Suite: managed by AMLC/FIOD, is a browser which combines FIU disseminations and legal information, depending on each organisation's needs and legal status (e.g. tax information for FIOD), with each other, and with open source information (e.g., Panama papers, Bahama Leaks) to detect signals/patterns of ML. Authorised officers (155 from FIOD and approximately 100 from the Police) can use the browser to perform searches and analysis.

JustisTRACK: can provide network drawings or information on possible abuse of legal persons, spontaneously and upon request (see IO.5).

Information Exchange on Counter Terrorism (CT Infobox): is a partnership between intelligence units, LEAs, OM and FIU-NL, headed by AIVD. It shares information on persons posing a terrorist threat. It works according to a closed box principle whereby the CT Infobox advises participating partners on the provision of information between them and the measures to be taken. It also draws attention to information that is available within the partners' own organisations.

Bank data referral portal: is a technical facility to automatically and centrally process the data of banks at the request of criminal investigative and prosecuting authorities and searches by FIU-NL and the Tax and Customs Administration. The portal enables LEAs to retrieve the requested information, including the BO information available in the data of banks (see IO.5).

134. In recent years, LEAs have increasingly requested iCOV reports to develop financial intelligence in the course of their investigations (see the statistics on iCOV usage in Tables 3.3 and 3.4 below). iCOV can generate new investigative leads by combining financial information to reveal assets related to a suspect and relationships between suspects, or other known criminals. A concrete example on LEAs' use of iCOV is included in Box 3.2. As a part of its in-depth analysis, FIU-NL also frequently requests iCOV reports to decide whether to declare a UTR suspicious and disseminate it to LEAs. The dissemination then becomes part of the iCOV reports by default, giving LEAs a holistic financial overview of the targets. LEAs in the BES Islands can submit requests to iCOV through the Netherlands Police or FIOD. They submitted a total of 15 requests between 2016 and 2021.

3

Box 3.2. Use of iCOV information by the Police

During an investigation into a possible violation of a police officer's integrity, the Police requested an income and assets report and a relationship report to iCOV. iCOV reports revealed that the officer had a connection with a large network of drug criminals through a personal relationship. The network report also uncovered a connection with a person working at another governmental agency, possibly involved in facilitating drug trafficking. The Police team expelled the police officer and shared the information about the drug-importing group with a special unit of the police for further investigation.

Table 3.3. Requests for iCOV reports

	2016	2017	2018	2019	2020	2021*
Number of requests	5 076	6 715	8671	14 454	16 150	14 621

* Covers the period up to 18 November.

Table 3.4. Requests for iCOV reports by agency

	2019	2020	2021*
Police	5 135	5 161	3 848
Tax Administration	2 325	2 984	3 147
OM	1 624	1 372	1 013
FIOD	1 033	1 124	1 351
FIU	640	1 416	1 003
Customs	23	21	18
CJIB	3 193	3 241	3610
DNB	19	16	18
Special Investigation Service ILT	44	60	37
Special Investigation Service ISZW	190	518	393
Special Investigation Service NVWA	50	67	59
Police Internal Investigation Department	108	114	97
ND Authority for Consumer and Markets	70	56	27
Total	14454	16150	14621

* Covers the period up to 18 November.

135. In addition to the information and reports available through the datahubs, LEAs can also separately consult other registers, such as the CoC, insolvency register, vehicle authority database or the land register. An essential source of financial information for LEAs is also their network of domestic and international partners. As described in IO.1, public-public and public-private partnerships are a key feature of the Netherlands AML/CFT system. LEAs also proactively engage their international counterparts through judicial and police-police MLA requests, as well as through Police/LEA/OM liaison officers to pursue cases with an international dimension (see IO.2).

Disseminations received and requested by competent authorities

136. FIU-NL produces and disseminates financial intelligence to LEAs, both spontaneously and upon request. FIU-NL receives a significant amount of information from obliged entities based on subjective and objective indicators. The below table provides a breakdown of UTRs reported to FIU-NL. The total number of UTRs in this table differs from Table 3.1, as some transactions were reported based on both subjective and objective indicators.

Table 3.5. The UTRs reported to FIU-NL from subjective and objective indicators

	2017	2018	2019	2020	2021*
Subjective UTRs (suspicions of ML/TF)	245 062	267 920	317 379	413 840	479 073
Objective UTRs (e.g., threshold reports)	117 524	119 109	217 233	308 165	621 632

* Covers the period up to 18 November.

137. FIU-NL has a wide range of powers to obtain information through direct and indirect access to several databases and datahubs. It has also frequently used its unique legal power to request information relevant for its analysis from all obliged entities to develop a complete financial intelligence picture and add value to its disseminations, in particular those triggered by FIU-NL's own investigation, LEA and foreign requests. The ability to process this extensive dataset is a key strength of the FIU, as it enables it to produce high quality analytical products for LEAs.

138. Customs (including in the BES Islands) submits all cross-border declarations and disclosures of currency and BNIs to FIU-NL, which are used in its analytical enrichment process. All declaration and disclosure information is integrated into the UTR database and can be used for future cross-matching (see Table 3.6). Approximately 7.5% of the Customs reports are included in FIU disseminations.

Table 3.6. Custom disclosures and declarations sent to FIU-NL

	2016	2017	2018	2019	2020	2021*
Customs (NL)	5 492	5 775	7 263	6 644	3 781	3 390
Customs CN (BES)	121	41	46	25	97	35

* Covers the period up to 18 November.

139. On a daily basis, the FIU-NL automatically screens all UTRs in its database against the Criminal Records (VROS) database and Central Fine Collection Agency (CJIB) register to identify any matches with subjects of ongoing criminal investigations, or with outstanding criminal fines. Positive hits result in the immediate automatic conversion of the UTR into a dissemination report to the relevant investigative, intelligence and security services.

140. The FIU-NL has also developed a system of queries to cross-check UTRs. Queries consist of specific themes, or key words used to automatically check and filter the large amount of information included in the UTR database. FIU-NL constantly refines and reviews queries based on the NRA, priorities of OM and LEAs, or any other identified risks to detect any new trends related to ML, TF or other offences. Whenever there is a match with a query, an automatic alert is generated and an analyst will perform a more in-depth assessment of the transaction(s) to determine whether it is appropriate to disseminate to LEAs.

141. FIU-NL also analyses requests received from foreign FIUs in the same way as domestic requests (see Table 3.1). While the TC Annex notes a minor technical deficiency under R.40, as there is no explicit legal basis for FIU-NL to exchange information with non-EU/EEA FIUs (outside of an MOU), this is not an issue in practice. Indeed, the FIU-NL regularly exchanges information, upon request or spontaneously, with foreign FIUs, including non-EU/EEA states. Information is exchanged via the established channel amongst EU FIUs (via FIU.net), which allows automated matching against subjects of interest. There has been an increasing trend in the number of FIU disseminations based on foreign requests, which is largely attributed to the digitalisation of FIU-NL internal procedures. However, in some cases the information transmitted by the FIU to its EU counterparts in the form of cross-border dissemination reports includes limited contextual analysis. FIU-NL provides further information and context to EU FIUs upon request (see IO.2).

142. The FIU-NL transfers its disseminations directly into LEAs databases. For example, FIU disseminations are exported into Blueview (the Police database) on a daily basis. LEAs, including the police and FIOD, have direct access to Blueview and therefore to FIU-NL disseminations. LEAs also consult iCOV and the AMLC Suite information hubs, which also contain FIU disseminations received on a weekly basis. The different frequencies in exporting FIU disseminations have only a minor impact on the timeliness and consistency of intelligence for LEAs' investigations, as LEAs, as a general practice, consult Blueview first when they are searching for FIU disseminations, and then iCOV and AMLC Suite as additional tools for both FIU disseminations and other relevant information for their investigative needs.

143. The case studies provided to the Assessment Team demonstrate an extensive use of financial intelligence in different types of investigations. The statistics on Blueview usage demonstrate an increase in the use of FIU disseminations by the Police (see Table 3.7 below). FIOD also regularly accesses dissemination reports as a standard practice in nearly all financial investigations. Indeed, approximately 60% of FIOD investigations include FIU dissemination reports.

Table 3.7. Number of dissemination reports consulted by Police in Blueview

	2016	2017	2018	2019	2020
Dissemination reports consulted by Police in Blueview	871	4 924	4 900	8 429	12 624

144. As there is no system in place to monitor follow-up action by LEAs, it is unclear how many FIU disseminations are left unattended in Blueview, particularly those deriving from FIU-NL's spontaneous disseminations. However, this is a minor concern considering the extensive co-operation between LEAs and FIU-NL, including joint ventures which ensure a timely hand-over and appropriate prioritisation of FIU disseminations. There is also no data to assess the full extent of FIU disseminations used in Police investigations into every ML or predicate offence. However, this is largely mitigated by the high usage of iCOV reports, and the exponential increase in Blueview usage by the Police to search for FIU disseminations during their investigations.

145. LEAs also seek financial intelligence from FIU-NL when no disseminations are available in Blueview. Such requests are sent through the OM and are referred to as "LOvJ" requests (see Table 3.8). These requests generally contain more operational details of an investigation. In 2020, over 50% of LOvJ requests originated from the Police, followed by FIOD and KMar. Based on the details of requests received, the FIU-NL conducts thorough analysis making use of its UTR database, and information requested from obliged entities, as well as from its international network and other available databases. In general, the FIU-NL responds to such requests within 21 days and there are often multiple dissemination reports generated for a single request.

146. BES Islands' authorities also submit LOvJ requests to FIU-NL, but to a significantly lesser extent. As noted under IO.7, there has been an increase in the resources allocated to BES prosecution and investigative services for ML and financial investigations. However, BES LEAs have limited capacity to analyse and process intelligence provided by FIU-NL in a timely manner (see also IO.7).

Table 3.8. LOvJ requests to the FIU-NL

	2016	2017	2018	2019	2020	2021*
LEAs NL	1 277	1 246	1 262	1 298	1 213	817
LEAs BES	3	5	1	4	1	3

* Covers the period up to 18 November.

147. FIU-NL registers the relevant predicate offence(s) for its disseminations (for both spontaneous disseminations, and those produced upon LEA requests). As noted in the below table, the vast majority of disseminations are related to ML with an unknown predicate (59%), followed by fraud (11%), corruption (7%), terrorism/TF/TFS (6%), human trafficking (6%) and hard drugs (4%). This is generally in line with the ML/TF risks in the Netherlands. Furthermore, half of TF investigations were triggered by FIU-NL's analytical products (see IO.9).

3

Table 3.9. Dissemination reports per predicate offences

Type of offence	2016	2017	2018	2019	2020	2021*	Total
ML	12916	15195	20939	19871	54231	36972	160 124
Terrorism/TF/TFS	3237	2204	2788	2101	3601	3148	17 079
Fraud	8304	3508	1583	2121	5964	7422	28 902
Hard drugs	3626	2540	1479	1585	578	1530	11 338
Other	640	828	329	145	698	538	3 178
Soft drugs	795	937	509	228	77	91	2 637
Human trafficking/smuggling	3874	1329	2462	4012	875	2141	14 693
Murder/homicide	987	635	400	199	170	290	2 681
Corruption	141	407	6194	316	9432	2268	18 758
Weapon trade	155	360	101	351	447	102	1 516
Synthetic drugs	580	213	54	111	373	320	1 651
Cybercrime	5	7	11	2	33	40	98
Child porn	388	27	284	1200	1640	1019	4 558

* Covers the period up to 18 November.

148. The continuous refinement and update of queries, technological developments and increase in FIU staff contributed to an increased number of disseminations in recent years. The FIU-NL also strived to maintain efficiency by keeping an average processing time for disseminations based on its own investigation under 30 days[35] between 2016 and 2021 (from 29 days in 2016 to 21 days in 2021). From an operational standpoint, this delay is reasonable and can be mitigated by the close co-operation between the FIU-NL and LEAs, as it allows the FIU-NL to prioritise urgent requests.

Operational needs supported by FIU analysis and dissemination

149. FIU-NL analysis and disseminations support LEAs operational needs to a very large extent. LEAs met during the onsite confirmed the long-established partnership and co-operation with the FIU-NL and the high quality of information provided by the FIU-NL.

150. As of November 2021, the FIU-NL employed 79 staff members, the majority of which (over 50) are financial and tactical analysts. 17 staff are in-house specialists for technological development. The FIU-NL has a permanent team of five analysts and one data scientist to conduct strategic analysis. One liaison officer operates in the BES Islands. FIU-NL conducts both operational and strategic analysis.

[35] This is the average processing time for FIU-NL's dissemination based on its own investigation, from the day a case file is opened to the day of dissemination.

Operational analysis

151. The FIU-NL can target LEAs' operational needs through its automatic interface with various databases. This allows for instant detection and dissemination of matches with subjects under ongoing criminal investigations in the Netherlands. Furthermore, the system queries are based on the ML/TF risks identified in the NRAs and the priorities of OM and LEAs (see Box 3.3). Other positive features include the direct and automatic transfer of FIU dissemination reports into the primary police database (i.e., Blueview) and the added value of having FIU dissemination reports in information hubs such as AMLC Suite and iCOV. As mentioned above, the increasing use of Blueview and iCOV reports is an indication of the utility of this information for LEAs.

Box 3.3. FIU intelligence in reacting to the COVID-19 emergency

In March 2020, the Dutch Government decided on a series of emergency allowances to react to the economic and social impact of the COVID-19 lockdown. FIU-NL made agreements with FIOD/AMLC, the Police and I-SZW, in co-ordination with the OM to detect possible fraud cases related to the use of COVID-related benefits. FIU-NL issued several newsletters to help obliged entities detect fraud, through specific characteristics and red flags. It also issued a special code for reporting UTRs related to possible COVID-19 fraud and put together a team to analyse any new coded UTR on a daily basis.

152. In addition to the FIU disseminations, the FIU also produces Financial Intelligence Reports (FIRs), spontaneously or in response to LOvJ requests. FIRs are in-depth analyses to depict complex transactions, networks, criminal activities and ML/TF patterns in criminal investigations. FIRs often contain hundreds of UTRs, as compared to FIU disseminations which may contain a smaller amount of UTRs. FIRs often serve as a package analysis to LEAs detailing a new ML/TF method and trend. The below table outlines the number of FIRs produced by the FIU during the assessment period.

Table 3.10. FIRs by the FIU-NL

	2016	2017	2018	2019	2020	2021*
Total	21	24	18	24	55	46
ML related	21	23	6	9	22	20
TF related	0	1	12	15	33	26

* Covers the period up to 18 November

3

153. Another direct tool for FIU-NL to respond effectively to LEAs' operational needs is to temporarily assign FIU analysts to investigative teams in charge of complex investigations into criminal organisations. Through this collaboration, FIU analysts can rapidly detect and provide disseminations upon demand and in line with operational needs. The below case study provides an example of such collaboration.

Strategic analysis

154. The FIU's Strategic Analysis Team is responsible for refining system queries and conducting thematic research to identify criminal trends and phenomena based on ML/TF risks, as well as LEAs' investigation priorities (see also IO.7). To provide some concrete examples, some of the queries seek to identify possible indications of human trafficking, ML via VAs, underground banking and corruption.

155. The FIU-NL also produces other types of strategic analysis, such as the formulation of new ML/TF typologies, mainly in co-operation with the AMLC and OM, and the issuing of binding guidance to certain types of obliged entities (e.g. the obligation for certain obliged entities to report specific elements or indicators to FIU-NL). The AMLC specifically scrutinises criminal investigations to detect new ML modus operandi, such as involving VAs. Based on an AMLC phenomenon description about bitcoin dealers, new ML typologies have been published on the FIU-NL website. The typologies also formed the basis of a new thematic ML project on VAs, initiated by FIU disseminations.

Box 3.4. Example of a FIR analysis

In 2016, FIU-NL analysed 75 transactions involving a total of over EUR 633 million through a bank account of a local company, carrying out illegal trust activities. The analysis identified a bank account in the Netherlands channelling funds from foreign individuals and entities listed in some international ML leaks and public scandals to other jurisdictions, including Kazakhstan, Liechtenstein, Estonia, UK, Israel, Switzerland, Czech Republic and Luxembourg.

The purpose of the transactions was to layer proceeds of crime through a third-party country. The operation and structure of the illegal activities was uncovered and detailed in a FIR after FIU-NL's extensive enquiries with foreign FIUs and consultation with other datahubs, such as iCOV and JustisTRACK.

Box 3.5. FIU participation in an investigative team

FIU-NL investigated UTRs concerning a purchase of a very expensive house. The suspect could not prove a legitimate source of income. Through additional information from obliged entities and foreign FIUs, as well as from the Blueview database, CoC and land registry, the FIU produced an intelligence report and transmitted it to the Criminal Investigative Team. The team involved the FIU throughout the investigation and the house searches. This close co-operation allowed the FIU to detect additional suspicious transactions. The suspect used a system of companies in the fruit trade and front men to mask money flows. Over EUR one million was transferred on the bank account of inactive fruit companies by a Dutch scrap dealer, allegedly for the payment for a large batch of scrap. At least 38 fictitious companies in the Netherlands and abroad were used to launder the money. Through a complex network of strawmen, accomplices and companies, the suspect was able to conceal his involvement and key role in the criminal network. FIU-NL reports enabled LEAs to gain further insight into a larger criminal network where the suspect was involved as a facilitator. This information led to follow-up investigations.

Co-operation and exchange of information/financial intelligence

156. As noted in IO.1, domestic co-operation and co-ordination is a key strength in the Dutch AML/CFT system, including at the operational level. This system is supported by extensive public-public, public-private and private-private partnerships. In terms of financial intelligence, the FIU has a central role in the majority of these structures. In the TF Platform, a public-private partnership, FIU-NL shares knowledge on themes, phenomena and typology with the four major banks and the Dutch Banking Association. It initiated the Fintell Alliance in 2019 (see Box 3.6) and takes part in the Asset Freezing Committee (see IO.10) and in the Consultation Team on Non-reporting Obliged Entities (see IO.1), as well as the Wwft Supervisors consultations (see IO.1 and 3). It is also a regular partner in the FEC initiatives, including the TF Task Force and Serious Crime Task Force, and a number of joint projects.

Box 3.6. Fintell Alliance

In 2019, FIU-NL set up the Fintell Alliance, a public-private partnership with four major banks. It aims to exchange financial intelligence and knowledge to improve the efficiency and efficacy of UTRs by banks. FIU-NL provides feedback, red flags and *modus operandi* to partnering banks to obtain information of higher relevancy and quality in return. This partnership is utilised in some operational platforms and thematic projects such as the TF Platform, TFTF, SCTF, FEC Project TBML and FEC Project Labour Exploitation.

Case example on the use of Fintell Alliance

In 2020, upon request from LEAs, FIU-NL investigated a ML scheme through underground banking by professional ML groups. By sharing information in Fintell Alliance, FIU-NL was able to detect a correlation that individual reporting institutions would not have been able to identify, based on their individual data. FIU-NL employees analysed their UTR database and conducted a joint analysis with Fintell Alliance institutions, which eventually mapped out an underground banking network and money flow involving more than 200 individuals, 200 bank accounts and 600 companies with a total value of suspicious transactions for over EUR 200 M. In addition to compiling a FIR for LEAs, the findings have been shared with banks and overseas counterparts to step up prevention and detection of underground banking.

3

157. The AMLC has a unique position in the national AML framework. It is housed under the FIOD and headed jointly by the FIOD and the Police. It provides a platform where all parties, both public and private, share their knowledge and expertise and work together at operational level for the verification of this knowledge and expertise (see also Box 3.1). Its staff of 40 includes a judge, who is a former prosecutor, ML experts, investigators and data scientists. Two AMLC employees work directly in the FIU-NL to further facilitate co-operation and access to information held by the tax administration. AMLC collaborates with the OM, FIOD, Police, FIU-NL, the Tax and Customs Administration, KMar and private sectors, and with international counterparts (through the Europe Financial Intelligence Public Private Partnership Steering Group) to facilitate ML complex investigations and to exchange knowledge on ML (see IO.7).

158. The frequent use of task forces, joint investigation teams and thematic investigation projects are also important tools to ensure that financial information and intelligence reaches the appropriate parties. The fieldlab approach is sometimes used for project-based co-operation led by the OM with participation of FIU-NL or other relevant parties. Fieldlabs examine a single offence, or a vulnerable sector, or a new phenomenon, which may present ML risks. At the regional level, the RIECs and LIEC also contribute to provide intelligence and analysis, in particular in co-operation with municipalities and provincial authorities, and regional and local police. The below case study provides an overview of a fieldlab initiative.

Box 3.7. Fieldlab human trafficking/smuggling

In 2018, FIU-NL participated in a fieldlab with the OM, the Police, KMAR, tax authorities and the Expertise Centre on Human Trafficking and Smuggling to detect possible transactions indicating sexual exploitation. The Fieldlab aimed at gaining insight into criminal networks exploiting women from Eastern Europe and worked together with an investigation team from RIEC. FIU-NL analysis identified multiple Romanian criminal networks. FIU-NL detected hundreds of money transfers to Romania, through specific queries and transmitted multiple case files to LEAs participating in the fieldlab. The transaction analysis exposed a financial pattern that was followed by the police to identify the network of facilitators.

159. There is a robust system in place to ensure the confidentiality of the financial information exchanged. The FIU-NL is physically located within the Police premises, with exclusive access to FIU staff, as verified by the Assessment Team during the onsite visit. UTR data is accessible only to FIU staff. There are also specific rules in the different partnerships to protect the information exchanged, including the use of anonymised information and secure channels. UTR data remains in the FIU database for a period of five years, while disseminations are retained for 10 years.

Immediate Outcome 7 (ML investigation and prosecution)

160. The Netherlands does not collect comprehensive data and statistics on the types of ML investigations and prosecutions, nor on the underlying predicate offenses. As a result, the Assessment Team relied heavily on the case examples provided by the authorities and onsite discussions with LEAs, prosecutors and judges to assess effectiveness.

ML identification and investigation

161. The Netherlands has a comprehensive legal and institutional framework to investigate and prosecute ML effectively. The Netherlands does not rely on the establishment of a predicate offence to prosecute ML and has a low threshold to initiate a ML investigation. It is sufficient to establish that an object is the direct or indirect proceed of an offence. Financial investigations are pursued systematically in criminal investigations both at the national and regional levels, in order to detect and confiscate criminal proceeds (see IO.8).

Overall conclusions on IO.6

1. LEAs use a wide range of financial intelligence to support their investigations into ML, TF and predicate offences, and to trace criminal proceeds. The FIU-NL is central to the production of financial intelligence based on the operational needs of LEAs and has a long-established operational co-operation with LEAs. It produces high quality operational and strategic analysis targeting LEAs needs and the ML/TF risks. The technological developments in the FIU have increased its capacity to analyse a large amount of data. There are minor concerns as to the unavailability of data on the usage of FIU's disseminations in Blueview and Police investigations.
2. In addition to the FIU products, LEAs increasingly request iCOV reports and engage AMLC, to gain a better insight into assets and networks of a suspect or a criminal group. Existing datahubs, public-public partnerships and public-private platforms are key features of the Dutch system and are regularly used in financial investigations.
3. The Netherlands is rated as having a high level of effectiveness for IO.6.

162. LEAs identify ML signals from a range of different sources, including datahubs. The Netherlands regularly uses financial intelligence from the FIU, as well as iCOV data intelligence reports, queries to AMLC Suite and JustisTRACK to detect ML signals and identify proceeds of crime. This conclusion is supported by the statistics provided in IO.6 on the use of FIU disseminations, and iCOV information by LEAs during their investigations. In addition to opening a ML investigation in parallel with predicate offence investigations, the Netherlands proactively initiates and pursues stand-alone ML. The authorities have prioritised thematic projects in accordance with ML risks, to detect new ML signals and schemes and develop ML typologies and indicators.

163. The authorities' proactive approach to identify ML offences and detect and confiscate criminal proceeds is reflected in the annual increase of ML investigations between 2016 and 2021 (see Table 3.11) and in the high number of stand-alone cases. Overall, since 2016, the Netherlands has conducted more than 17 200 ML investigations, of which over 10 100 are standalone. The majority of ML investigations have been conducted at regional level (approximately 15 300 cases).

164. Cases initiated at the national level as a result of thematic projects are complex and include the prosecution of different forms of ML. Since 2016, 2 785 investigations have been launched at the national level by the FP and LP. Due to the low threshold to initiate a ML investigation, regional cases tend to be less sophisticated, with a majority involving self-laundering. However, case studies demonstrate that regional investigations also include complex stand-alone or third-party ML cases, and criminal investigations into predicate offenses where ML risks are high (i.e., drugs and fraud offenses).

Table 3.11. Overall number of ML investigations conducted at regional and national levels

	2016	2017	2018	2019	2020	2021*	Total
Police	1 589	1 766	1 932	3 040	3 589	2 789	14 705
KMar	180	146	93	143	175	50	787
BOD (incl. FIOD)	297	290	268	297	248	134	1 534
Other	36	48	33	71	48	16	252
Total	2 102	2 250	2 326	3 551	4 060	2 989	17 278

* Covers the first half of the year.

165. The OM plays a major role in the investigation and prosecution of ML. Three different offices handle ML cases:

- The *National Public Prosecution Office for Serious Fraud, Environmental Crime and Asset Confiscation* (OM/FP) is a specialised office responsible for economic offences, complex ML and confiscation cases. Within the FP, a dedicated ML National Public Prosecutor (LOvJ for ML) is responsible for coordinating ML policies throughout the country and promoting the transfer of knowledge between all parties involved in ML investigations (e.g., FIOD, Police, FIU-NL, the LP and the APs). The OM/FP works in close co-ordination with FIOD and other specialised LEAs (BODs) (see R.30).
- The *National Public Prosecution Office* (OM/LP) focuses on ML related to national and international organised crime, including human trafficking and drug trade, and works closely with the Police and its Central Criminal Investigations Division.
- Finally, the *District Public Prosecution Offices* (APs) manages local/regional ML cases, in co-operation with regional police units.

166. All LEAs involved in ML investigations have financial expertise and continuous training available as well as dedicated teams to work on complex financial investigations.

Table 3.12. Role of main LEAs involved in ML investigations

Agency	Specialist units and resources	Responsible OM office	Type of ML cases pursued
Police	10 regional units All units have in-house financial investigators. Specialised financial expertise teams (FinSup) support complex financial investigations at regional level 1 Central unit with a Central Criminal Investigations Division (DLR). Three specialised financial criminal investigation teams (FinEC) support DLR work on complex ML cases. In National Police total: 65,000 employees. 773 financial investigators and 203 financial intelligence experts in the regional units. 159 financial investigators and 21 financial intelligence experts in DLR.	OM/LP or APs for regional/ local cases.	Regional units: - ML cases at the regional level (drug offences or other criminal activities, mainly self-laundering). - complex ML cases involving regional elements and support to financial investigations of regular teams DLR: complex ML cases linked to organised criminal groups, with a national or international dimension.
FIOD	13 offices in six regions. 1627 staff, of which 1 463 financial investigators	OM/FP	Stand-alone ML cases and complex ML cases related to tax crimes, fraud, corruption or other economic offences.
KMar	National brigades (5 000 operational staff) divided in tactical, specialist, and financial and economic teams (28 FinEC staff, 10 staff in SVLM-see IO8)	AP	Regional ML investigations at the borders, including at Dutch international airports.

167. Within this general repartition of tasks, the OM can opt to assign a case to a joint Police and FIOD investigation team, notably for investigations involving complex financial or economic schemes, and serious organised crime. The national Combined Team exploits the specific knowledge and expertise of both LEAs. The Combined Team investigations are usually longer, due to the complexity of the schemes, and often involve co-operation with international partners. An example of Combined Team investigation is presented in Box 3.8. The OM can also assign an investigation to the MIT (see IO.1).

3

Box 3.8. Example of ML investigations by different LEAs

ML investigation conducted by the Combined Team

In 2018, the Combined Team initiated a complex investigation into TBML and underground banking. It originated from STR disseminations by FIU-NL that revealed considerable amounts of transactions in the trade of onions and potatoes with West African countries were settled in cash, for an amount of over EUR 150 million over the period 2014-2019. The money was moved through underground banking. The traders in the Netherlands accepted payments in cash over EUR 10 000 without fulfilling the obligation to report them as per the Wwft. The investigation, which is ongoing, is examining at the role of underground bankers and cash-couriers, who are suspected of laundering criminal funds through these cash transactions.

Complex ML investigation conducted at regional level

In 2018, a local investigation team in the Hague regional police unit started a ML investigation after five Kg of cocaine and EUR 60 000 in cash where found in a drug dealer apartment. The team was supported by the Police's regional FinSup and FinEC teams. Since the drug dealer was not registered at that address, the investigation tried to identify who was paying the rent. The investigation revealed constructions set up to hide the criminal identity of the tenants through legal real estate infrastructures, the use of the properties for criminal activities and the laundry of illicit money through rent payments. The main suspect's company introduced criminal tenants to two real estate investors. He was receiving the rent in cash and transferring it to them. In 2019, 34 house addresses were searched and almost eight million EUR in cash and 25 cars were seized, as well as drugs, weapons and PGP phones. In 2020, five suspects were convicted for habitual ML to imprisonment sentences ranging from 28 months to five years.

168. The most complex ML cases are discussed by the Steering Team. A Consultation Team carries out a preliminary evaluation of the ML signals against the main ML risks and the AML Strategic Programme and presents the most important cases to a Steering Team. The Steering Team includes representatives from the OM (FP and LP), the Police and FIOD, and decides on launching ML investigations and assigns the case to a specific LEA (at regional or national level) or the Combined Team. High-end ML cases are usually conducted at national level. An example of a complex case handled at regional level is presented in Box 3.8 above.

Table 3.13. ML investigations initiated by the Steering Team

	2016	2017	2018	2019	2020	2021*	Total
FIOD/FP	64	101	95	77	66	50	453
DLR/LP	20	16	40	32	33	19	160
DLR FinEC team dealing with ML and cash	n/a	4	17	17	11	9	58
Combined Team	11	14	14	11	6	2	58
Total	95	135	166	137	116	80	729

* Covers the period up to 1 October.

169. Since 2016, the Steering Team initiated over 700 investigations, as shown in Table 3.13. The increasing complexity of the cases and criminal schemes, as well as the frequent need to request MLA in these investigations, explain the slight decrease in the overall number of investigations that the Steering Team initiated annually.

170. The case studies on ML project-based investigations and investigations deriving from the Steering Team show a high level of financial expertise, especially through the involvement of various specialised investigative services. LEAs use a wide range of investigative techniques in the course of their financial investigations. Information obtained through iCOV, JustisTRACK and AMLC Suite is regularly included in the investigation file and can be used as evidence in Court. Where needed, a criminal financial investigation (SFO) can also be instituted, providing powers to prosecutors and investigative officers in obtaining documents and seizing evidence and assets in the consecutive confiscation process. The below case study highlights a case initiated by the Steering Team.

Box 3.8. Example of complex ML investigation involving an online bitcoin mixer

In 2018, the authorities received information from a cyber-security company that a bitcoin mixing service was operating in the Netherlands. The mixer was splitting up and reassembling virtual currencies to make them untraceable, against the payment of a commission. The joint investigation by FIOD (and its specialised cyber team FACT), the AMLC and the Police (High Tech Crime Team) led to dismantling one of the largest online mixers for VAs, which was used to launder criminal money. The authorities estimated that the mixer achieved a turnover of at least USD 200 million per year. The Netherlands cooperated closely with EUROPOL, Luxembourg and other EU countries. Six servers were seized in the Netherlands and Luxembourg. FIOD collected and analysed all customers and transactions data in the server and shared relevant information with other countries.

171. During interviews with the authorities, a challenge emerged in relation to obtaining information protected by the legal professional privilege in a timely manner. The authorities initiated several steps to process and decide cases where the legal professional was invoked in Courts after the seizure of evidence, but it continues to be an issue. Almost all ML complex investigations by FIOD require evidence held by lawyers, notaries, or other (legal) professionals. In order to access this evidence, the OM must submit a request to an investigative judge, and then to the Court and possibly the Supreme Court, as the defence often invokes legal privilege regarding the seized information. In practice, the entire process takes a considerable amount of time: an average of 211 days for examination by the investigative judge; 346 days to be discussed in Court; and 269 days to reach the Supreme Court. According to experts met during the onsite, this time-consuming process has in some cases resulted in delays in investigations and prosecutions, and reduced sentencing for ML because of breaches of the undue delay principle. No statistics on the frequency of undue delays breaches are available, as this issue is not always specifically mentioned in the final sentencing by the judges.

3

172. The OM retains the sole responsibility for the prosecution of offences, including ML. It has discretionary power to decide whether to prosecute a case or settle it out of court (see Table 3.14). Since 2016, the OM has unconditionally dismissed 35% of the ML investigations, due to the unlikeliness to achieve a conviction, or discretionary or administrative dismissal. An increasing number of cases have also been settled out of court. Several factors can explain these figures. For example, the low evidentiary threshold to initiate a ML investigation (a reasonable suspicion that the money is of illegal origin, without the need to identify a specific predicate offence) entails that a high number of cases cannot be proven after further investigation. In approximately 70% of the dismissed cases, there was insufficient evidence to proceed to court, or insufficient national interest (for instance, in cases where the same individual is already part of an investigation abroad). Overall, between 2016 and 2021, approximately 53% of the ML investigations resulted in ML charges presented to the courts. The OM concluded approximately 10% of the investigations by imposing out of court settlements or penalty orders (see further for an analysis of the sanctions imposed). Amongst the ML cases presented to Court (both mixed and stand-alone), the conviction rate for ML cases concluded in the first instance is positive, and close to 62%. Table 3.15 presents an overview of the final Court decisions, in the first instance (i.e. cases where there was no appeal). The overall conviction rate is higher (80%) when considering all ML convictions in the first instance (i.e., including also those cases that are not final and for which an appeal has been submitted).

Table 3.14. Assessment of ML cases (both mixed and stand-alone, national and regional) by the OM

OM decision	Explanation	2016	2017	2018	2019	2020	2021*	Total %
	Total decisions by OM	2016	2136	2514	3383	4321	3335	17 705
Summoning	The case is sent to the Court	1248	1201	1395	1801	2119	1581	9 345 *52.8%*
Unconditional dismissal (of which, unlikelihood of conviction)**	OM decision to dismiss a case (of which, for insufficient evidence)	539 (339)	687 (468)	847 (563)	1242 (933)	1685 (1242)	1255 (981)	6 255 (4 526) *35.3%*
Conditional dismissal	Specific conditions are set up by the OM to dismiss the case	17	24	28	56	114	115	354 *2%*
Out of court settlements or penalty orders	Non-trial resolutions, either through an agreement with the offender, or by imposing a penalty order	200	205	224	262	386	378	1 665 *9.4%*
Others	Cases joined together, de-registration, transfer to use other type of measures (e.g. administrative, fiscal, disciplinary)	12	19	20	22	17	6	96 *0.5%*

* Covers the first half of the year.
**Unconditional dismissal also includes cases where the suspect was unable to go to Court (e.g. death) or case of insufficient national interest (e.g. foreign proceedings ongoing).

Table 3.15. Final ML convictions in stand-alone and mixed cases for natural and legal persons in first instance

	2016	2017	2018	2019	2020	2021*	Total (of which legal persons)
Court cases where ML was charged (legal persons)	891 (25)	1054 (6)	1163 (40)	1480 (23)	1437 (18)	1047 (13)	7 072 (125)
Number of ML convictions** (legal persons)	493 (14)	611 (3)	726 (27)	928 (10)	939 (9)	689 (3)	4 386 (66)
ML convictions (%)	55.3%	58.0%	62.4%	62.7%	65.3%	65.8%	62%

* Covers the first half of the year.
**This number refers exclusively to cases where the ML offence was proven.

ML identification and investigation in the BES Islands

173. In recent years, the Netherlands has invested significantly in strengthening the capacities of the OM BES office to handle ML cases, and has set up a specialised ML Public Prosecutor within OM BES office.[36] Moreover, the KPCN has started trainings to increase its expertise on financial investigations and added cyber experts to its force. The RST has also been deployed locally, to ensure closer co-operation with the KPCN. The OM BES cooperates closely with the KPCN and with RST to handle investigations. In practice, for ML investigations, the KPCN is heavily reliant on the capacity and expertise of the Netherlands Police and the police from Aruba, Curacao and Sint Maarten. The RST—a partnership between the police forces in the Kingdom, including FIOD staff members based in Curacao—is often deployed to deal with serious organised crime.

174. While KPCN is working on enhancing its financial expertise on ML and financial investigations, this is a recent development and will require additional resources and continuous commitment from the authorities. LEAs in the BES Islands have access to FIU-NL disseminations and can submit requests for FIU-NL information through the OM BES. KPCN has no direct access to intelligence hubs used in continental Netherlands, as the BES Islands and continental Netherlands form different legal jurisdictions. When necessary, KPCN can obtain intelligence from European Netherlands, through MLA and police-to-police co-operation.

175. Similar to continental Netherlands, a Steering Group with representatives from OM BES, KPCN and KMAR decides whether to launch ML investigations. As shown in Table 3.16, between 2016 and 2020, LEAs initiated 41 ML investigations, and in all cases a predicate offence was involved. One case was settled by OM BES and 14 were brought to trial, with ML convictions achieved in nine cases. Box 3.10 provides an example of a ML investigation carried out in the BES Islands. The majority of ML cases in the BES Islands involves an international component. LEAs reported challenges obtaining relevant information from other countries in a timely manner.

36 At the time of the onsite visit, the ML prosecutor in the OM BES was in the process of drafting a ML Action Plan to guide the investigation and prosecution of ML cases, but also the development of prevention mechanisms.

3

Table 3.16. ML cases in the BES Islands

	2016	2017	2018	2019	2020	Total
Inflow of cases to OM BES	14	6	3	15	3	41
OM BES decision on the outcome of the ML investigation						
Unconditional dismissal	2	3	1	3	-	9
Conditional dismissal	3	2	2	10	-	17
Settlement	-	-	-	1	-	1
Convictions on ML cases						
ML convictions	1	-	2	1	5	9

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

Box 3.9. Example of a ML investigation in the BES Islands

Between 2019 and 2020, KPCN investigated the illegal granting of loans by unlicensed individuals, on a large scale and against payment of usurious interests. KPCN cooperated closely with AFM and DNB, due to their supervisory role on financial companies in the BES Islands. The investigation used FIU-NL disseminations to gain insights into the financial position of the suspects. The investigation revealed that almost USD 500 000 was lent in the period from 2018 to October 2019. While one suspect was convicted to three months imprisonment for violations of several provisions of the Financial Market Act BES (Wfm BES), the person was not convicted for ML.

176. The national AML Strategic Programme 2019-2022, coordinated by the LOvJ for ML, identified six priority themes to guide ML investigations, aligned with the 2017 ML NRA findings. In addressing these priorities through operational activities, LEAs also integrate the most recent findings of the 2019 ML NRA, and any trends or recent developments identified during ML investigations, new typologies or indicators. Box 3.11 outlines the six main themes pursuant to the AML Strategic Programme. As noted under IO.1, the authorities' approach to assessing ML risks focused mainly on the methods and channels, rather than on the identification of the main predicate offences. The same approach is reflected in the Strategic Programme.

Box 3.10. The six themes under the Programme AML 2019-2022

1. **Concealed assets**: tracing criminal assets entering the legal economy, mainly through fraud.
2. **Non-reporting obliged entities**: prosecuting obliged entities failing to comply with Wwft obligations.
3. **Illegal service providers**: identifying professional money launderers and facilitators.
4. **Means of payment**: identifying ML methods related to VAs or the use of cash.
5. **TBML**: using national and international flows of goods and commodities to disguise ML.
6. **National and international investments in companies/funds**: using national and international investments in companies/funds to launder money.

177. The Netherlands makes extensive use of thematic investigation projects to enhance knowledge on ML schemes and identify ML signals. The projects are often started based on specific investigations. The increased knowledge acquired during a project allows LEAs to detect new ML signals and initiate new investigations.

178. There is a strong correlation between the topics of the projects, the NRA ML risks and the themes identified in the national AML Strategic programme. Previous thematic projects occurring prior to the assessment period contributed to the identification of the six priority themes of the 2019-2022 AML Strategic Programme and generated a considerable number of ML investigations conducted within the assessment period (see box 3.12). For example, in relation to the topic of concealed assets, in 2015, the AMLC initiated a debit/credit cards project to detect possible ML, including ML associated with tax fraud, through the analysis of foreign debit/credit cards used in the Netherlands by Dutch residents, and which revealed unknown and undeclared foreign bank accounts. Moreover, between 2014 and 2016, FP and FIOD conducted a voluntary disclosure project to investigate whether the assets declared as part of a voluntary disclosure scheme had a possible illegal origin. Between 2014 and 2015, FP, FIOD and the Tax and Customs Administration conducted a project on suspected income tax evaders, to analyse mismatches between luxurious lifestyles and declaration of incomes. Finally, since 2018 the offshore project has aimed at gaining insights into the possible use of offshore companies or legal arrangements to purchase immovable property in the Netherlands and identify related ML schemes.

179. Between 2012 and 2017, a project on non-reporting obliged entities focused on criminal enforcement of the AML/CFT violations to improve compliance amongst obliged entities. It resulted in the opening of 73 criminal files, and 36 out of court settlements or convictions. In relation to payment means, the AMLC led projects on VAs (2016-2018) and VA mixers (2019-ongoing) used to launder money, which focused on developing typologies and indicators with the FIU, based on several investigations carried out by LEAs. Finally, in 2018, the FEC initiated a public-private project to develop further knowledge and expertise on TBML and identify signals, based on the TBML cases investigated by the authorities.

3

180. The Netherlands does not maintain comprehensive statistics on the underlying predicate offences for ML investigations/prosecutions/convictions, limiting the assessment team's view of all ML cases pursued by the authorities. However, the Netherlands provided sufficient cases to demonstrate the consistency between ML investigations and the thematic risks and priorities of LEAs. Box 3.12 includes some examples.

Box 3.11. Consistency of ML investigations with ML channels and methods identified in the NRA

Investigation into major compliance failures by a bank

Based on signals emerging from the non-reporting entities project, in 2016 the OM opened a criminal investigation into multiple, structural failures by a FI to perform appropriate client controls and accounts monitoring over a long period of time (2010-2016), which resulted in those accounts being used for ML and criminal activities. The FI accepted to pay an out-of-court settlement of EUR 775 million offered by the OM for structural violations of the Wwft and culpable ML. In 2020, the Court of Appeal ordered the OM to prosecute the FI CEO due to his failure to take measures to prevent the FI criminal conduct.

Investigation into ML through bitcoins

In 2017, the FIU-NL identified an individual at the centre of a criminal network with EUR 1.4 million in transactions related to bitcoin traders. Based on a FIU-NL dissemination, FIOD started a criminal investigation into the suspect. The investigation of the blockchain analysis revealed that the bitcoins were associated with illegal transactions on the darkweb. The subject was offering services to convert bitcoins into cash. Bitcoins owners were transferring bitcoins to the suspect's wallet or to the wallets of bitcoin sales companies. The suspect was then transferring the corresponding amounts to his own bank accounts, as well as the accounts of associates. Transfers for a total amount of EUR 447 882 were made. The suspect withdrew most of this money in cash and provided it to the bitcoin owners within 24 hours. In 2017, he was convicted for habitual ML to 12 months in prison (and eight under probation). The Court ordered a value confiscation of EUR 142 013, corresponding to his unlawfully obtained benefit.

Investigation on ML through international investments

Between 2015 and 2018, the OM/LP conducted an investigation into a Dutch individual who invested cash in portfolios registered in the name of offshore companies in Panama. The subject had worked in Swiss banks, and then started working as an independent asset manager. The suspect had clients with criminal antecedents and clients with undeclared savings, who probably wanted to keep their income or assets out of the sight of the LEAs and tax authorities. The investigation also revealed that the suspect dissipated part of the money from his clients for personal purposes. In the course of the investigation, the LP submitted MLA requests to Switzerland, Liechtenstein, Dominica and Panama. The suspect was arrested in 2018 while transiting in the Netherlands. In 2021, he was convicted for habitual ML, forgery, embezzlement and fraud to eight years.

181. As evidenced by the thematic cases presented, the Assessment Team concludes that the AML strategic programme and the thematic projects reflect the main ML risks faced by the Netherlands. Furthermore, the LEAs met during the onsite visit confirmed that drug trafficking and fraud were the most common predicate offences encountered in their ML investigations. At regional level, the RIECs play an important role in ensuring that LEAs focus their efforts on the prevailing proceeds-generating offences and regional risks when investigating ML and organised crime.

182. ML investigations in the BES Islands are scarce and do not fully reflect the ML risks. The limited case examples provided by the authorities show that financial investigations in most of the cases did not result in the formulation of ML charges. The authorities have so far focused most of their efforts on the prosecution of predicate offences, and the confiscation of proceeds of crime.

Types of ML cases pursued

183. The Netherlands does not collect statistics on the types of ML investigated and prosecuted. However, based on the analysis of case studies and interviews with the authorities, the Assessment Team found that LEAs pursue a wide range of ML investigations, from self-laundering to complex cases involving offshore companies, professional money launderers and VAs, as illustrated in Boxes 3.12 and 3.13. The authorities have pursued and convicted offenders, both for complex and simple ML cases and for stand-alone ML, without the need to establish a link to a specific predicate offence.

Box 3.12. LEAs' ability to pursue different types of ML

Stand-alone ML: In 2016, Customs and FIOD investigated a suspicious intended shipment of an ambulance and a car from the Netherlands to Suriname and found hidden parcels of cash for a total of EUR 2 million in EUR 500 notes. The banknotes were packed with ground coffee, which is regularly used by smugglers to evade tracking dogs. LEAs found evidence that the suspect was aware of the hidden cash. The suspect was unable to provide a concrete and verifiable statement on the origin of the money. The Court concluded that the cash was directly or indirectly deriving from criminal activities and in 2018 sentenced him to 2.5 years imprisonment for ML and forgery. The EUR 2 million cash and ambulance were confiscated.

Third-party ML: This investigation started in 2016, on the basis of residual information from an earlier investigation into a corrupt Customs officer who was bribed to allow large quantities of cocaine to be imported in the port of Rotterdam. The authorities examined the role of a facilitator, a former assistant auditor who put the corrupted custom officer on a fictitious payroll of an employment and secondment agency to launder the money. The fictitious salary was paid through funds coming from a Liechtenstein bank account, in the name of a Panamanian legal entity and managed by a Russian proxy. The assistant auditor had also used real estate purchases to launder the money, and facilitated the deposit of money into the account of the Russian proxy to purchase a luxury car worth EUR 87 000 via a foreign construction. In 2018, he was sentenced to four years imprisonment for habitual ML of EUR 307 561 (the fictitious salary), EUR 410 000, EUR 852 050 and EUR 87 500 (for the purchase of two houses and a luxury car).

ML from foreign predicate offence: Three private companies laundered EUR 11 million through the purchase of real estate in the Netherlands and Germany. The companies were controlled by a Dutch foundation and a Dutch holding, managed by a TCSP that was a suspect in an investigation. The BOs were individuals convicted in Russia for stealing money from their banks. They purchased the real estate via a concealing arrangement in order to launder the money. The funds were transferred to the three Dutch private companies via a Danish and a Swiss bank. The investigation is ongoing. OM seized the real estate in the Netherlands and Germany, as well as the bank accounts of the suspects.

Self-laundering: A doctor received payments from the pharmaceutical industry to test new drugs and deposited them in his Luxembourg bank accounts. The suspect never declared the balances of these accounts - and thus the income and capital received - in his income tax returns. In 2016, the investigation revealed that he had withdrawn over EUR 3 million in cash from the Luxembourg bank accounts over a ten year period to hide such payments. He was convicted of habitual ML and deliberately filing tax returns incorrectly or incompletely to a term of imprisonment of 15 months and a fine of EUR 500 000.

184. In the BES Islands, ML investigations have so far been pursued only in conjunction with a predicate offence. Over the reporting period, only nine ML convictions were achieved, which suggests the limited ability of BES LEAs to pursue and prosecute different types of ML, in particular stand-alone ML investigations.

Effectiveness, proportionality and dissuasiveness of sanctions

185. The Netherlands' approach to criminal sanctions focuses on a combination of prevention and repressive measures, as well as prioritising confiscation. When sanctions are imposed, these can take the form of a fine, conditional/unconditional imprisonment and/or community service. The authorities consider that the preventive approach is equally, if not more important than repression. However, the Assessment Team is concerned by the low level of ML sentences imposed in practice, including in serious and complex cases.

186. The maximum penalty for ML is a term of imprisonment of six years, which can increase to eight years in case of habitual ML, or a fifth category fine. In addition, community service of up to 240 hours can be imposed. For legal persons, the fine can increase up to a maximum 10% of the annual revenue. No concurrent sentences are allowed. When the Court sanctions ML in combination with other offences, judges apply a single combined sentence for all crimes. In such cases, it is not possible to draw a distinction between the penalty imposed for ML and the one imposed for other offences, or to assess the extent to which the ML charge led to a higher sentence.

187. The Netherlands does not maintain comprehensive statistics on the sanctions imposed in ML cases. The information provided has been extracted manually, and is limited to aggregated statistics on the average sentences in ML cases. The sanctions imposed vary according to the complexity of the cases. However, based on this limited data, it is not possible to distinguish between the level of sentencing imposed in simple ML cases (e.g., self-laundering) and in more sophisticated cases. Accordingly, the Assessment Team considered the case studies provided by the authorities to gain additional insights into sanctions imposed, and held discussions with judges and prosecutors in the course of the onsite visit.

188. The actual average of sanctions (prison sentences and fines) imposed to natural and legal persons in ML cases is very low and well below the legally prescribed maximum limits. In practice, the Netherlands has imposed, on average, prison sentences of less than a year in stand-alone cases and between one and two years in mixed cases involving other offences. This average data includes both the unconditional prison term, and the part of the sentencing that is suspended under probation. As a result, the actual level of unconditional prison sentences is lower than it appears in the table 3.17 below. While this low average can be partly explained by the higher number of simple ML cases, the review of the case studies provided confirms that sanctions imposed in many complex and mixed cases are generally on the lower-end of the scale and not dissuasive.

189. Furthermore, the average fines imposed to natural and legal persons are well below the legally prescribed maximum limits (see Table 3.18), which affects their dissuasiveness especially if they are applied as the only sanction. The figures included in the table do not distinguish between conditional and unconditional fines imposed.

Table 3.17. Average prison sentence imposed in stand-alone and mixed ML cases (first instance)

	2016	2017	2018	2019	2020	2021*
Stand-alone ML cases						
Total prison sentences (days)	177	143	193	144	154	147
Combined sentences in mixed cases						
Total prison sentences (days)	646	697	636	580	579	503

3

Table 3.18. Average fines imposed on natural and legal persons

	2016	2017	2018	2019	2020	2021*
Stand-alone ML cases						
Number of cases (natural persons)	12	16	29	35	30	27
Average sanction (natural persons, in EUR)	12 502	8 868	3 678	9 940	3 694	1 227
Number of cases (legal persons)	3	2	15	6	7	2
Average sanction (legal persons, in EUR)	35 000	10 000	21 267	27 500	176 929	375 500
Mixed cases						
Number of cases (natural persons)	6	14	19	19	15	11
Average sanction (natural persons, in EUR)	7 920	16 775	31 514	34 069	5 599	41 721
Number of cases (legal persons)	11	1	12	4	2	1
Average sanction (legal persons, in EUR)	13 005	20 000	126 992	95 590	25 000	180 000

* Covers the first half of the year.

190. Overall, in the view of the Assessment Team, the low level of ML sanctions affects their dissuasiveness. As noted in R.3, the Netherlands applies the *una via* principle, whereby it is impossible to impose both criminal and civil/administrative sanctions for the same offence. Furthermore, the possibility to totally or partially suspend the prison terms and to replace it with a fine or community service further reduces dissuasiveness.

191. The OM developed ML prosecutorial sentencing guidelines to determine the proposed sanction it refers to the Court. The judges are not bound by the OM proposals and have discretionary powers to assess each individual case. Unlike prosecutors, they are not guided by specific ML orientation points (i.e., sentencing guidelines). In practice, for ML cases they use sentencing points of reference for economic and financial crimes, such as fraud. However, the fraud guidelines give a prominent role to the actual gain of the suspect, rather than to the complexity of the cases, and often result in lower sentences being imposed. The breach of the undue delay principle, due to the excessive length of the investigation or prosecution, is another element that is taken into consideration by judges and can often lead to lower sentences. The authorities highlighted that the long duration of ML cases is also related to some capacity/resource issues for judges, and to a lesser extent, for prosecutors. The Netherlands was unable to provide statistics on the impact of the undue delay principle on ML sentencing.

192. The Assessment Team also notes that in most cases provided by the authorities, the sentences were not final. Assessors were provided with the numbers of appeals lodged but did not receive information on the result of the appeals nor the average success rate in achieving final convictions upon appeal.

193. ML sanctions provided in the BES Criminal Code are high, with a maximum sentence of 12 and 16 years' imprisonment for ML and habitual ML, and/or a fifth category fine. However, the sanctions imposed in practice in the nine mixed ML cases are much lower, with the highest fine being one year of conditional imprisonment for embezzlement and ML of USD 300 000. In most cases, only a pecuniary sanction and a few months of suspended prison term was imposed.

Use of alternative measures

194. The Netherlands can apply alternative criminal justice measures. The decision to prosecute a case for ML, or for a different criminal charge lies with the OM. This discretionary power is part of the OM prosecution policy, and it is not limited to cases where it is not possible to secure a ML conviction. In the presence of an identified predicate offence, the OM could opt to prosecute for the underlying offence and the confiscation of proceeds of crime, despite the suspicion of ML, in case of justifiable reasons. In addition, the OM can also decide to settle a case out of court. The out of court settlements establish certain conditions for the suspect, such as the imposition of fines, confiscation measures, or the acknowledgement of the statement of facts. The Prosecutor can also opt to impose a penalty order to end a case. If the suspect does not agree with the penalty order, a judge will assess the case. The authorities consider these types of settlements as a form of prosecution and have made frequent use of these measures (see table 3.14).

195. In addition, the OM can also decide to share information on a case with supervisory authorities, for a fiscal or administrative settlement with a penal element when a criminal approach is not opportune or a fiscal, disciplinary or civil settlement is more efficient. The Netherlands considers the failure to meet Wwft obligations as a criminal offence. The Economic Offences Act allows for an alternative approach in cases where ML prosecution is not possible, and has a lower burden of proof than a ML charge.

3

Overall conclusion on IO.7

The Netherlands successfully detects and investigates ML signals and prosecutes different types of ML through the systematic use of financial intelligence and investigations and the strong co-operation between LEAs. The AML Strategic Programme, and the thematic investigation projects provided by the authorities are strengths of the Dutch system. The Netherlands does not maintain comprehensive statistics on the underlying predicate offences for ML investigations/prosecutions/convictions, limiting the assessment team's view of all ML cases pursued by the authorities. However, case examples provided on national and regional investigations are consistent with the ML channels and methods identified in the NRAs. Although the Netherlands has a high conviction rate, the low level of sentencing imposed partly frustrates the proactive efforts of the authorities to prosecute ML. The increasing resources allocated to the prosecution of ML in the BES Islands are a welcome step, but further efforts are needed to develop LEAs' capacities to undertake ML investigations.

The Netherlands is rated as having a substantial level of effectiveness for IO.7.

Immediate Outcome 8 (Confiscation)

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

196. The confiscation of criminal proceeds is a high priority for the Dutch government. This conclusion is based on the consideration of strategic documents, operational initiatives undertaken by the authorities in recent years, and interviews with relevant stakeholders during the onsite visit. The authorities consider depriving criminals of their assets to be equally, or even more dissuasive, than imprisonment. LEAs and government policies, strategies and guidance consistently focus on depriving criminals of their proceeds, and tackling the criminal business model as a top priority.

197. At a policy level, confiscating criminal assets is an annual priority within the budget of the Ministry of Justice and Security. The 2019-2022 Agenda of the Ministry of Justice and Security also recognises the importance of a financial angle to tackle subversive crime. This includes, in particular, the use of financial investigations to: identify money flows, uncover financial structures, and ultimately disrupt the criminal revenue model; collect evidence in criminal investigations; confiscate all criminal profits, and support compensation for victims.

198. This policy priority is also reflected in the OM Confiscation Instruction (and in the similar Confiscation Instruction in place in the BES Islands), which requires all LEAs to conduct a financial investigation into criminal assets and money-flows as a standard procedure in all criminal investigations. Within the OM, a National Confiscation Coordinator (LCA) acts as strategic advisor on the national confiscation portfolio. The LCA is responsible for developing policies in this area, but also ensuring their operationalisation within the OM.

199. In 2019, the OM reviewed the confiscation strategy for the Police, FIOD and OM ("Intensifying the focus on criminal money flows"). The main development was the setting-up of a Steering Committee for Confiscation, with representatives from the three institutions. The Steering Committee for Confiscation meets three times per year to assess and coordinate the implementation of confiscation measures. Another core action under the strategy is training and continuous learning to increase LEAs' ability to deal with complex ML cases, and the adoption of a multi-disciplinary approach to make use of the most effective instruments available under criminal, administrative and tax law. Finally, the confiscation strategy highlights the importance of international co-operation, to enhance asset sharing and facilitate cross-border confiscation.

200. The priority attributed to confiscation has also resulted in additional resources allocated to the OM and LEAs, to enhance the authorities' ability to seize and confiscate assets. Within the OM, every department has a dedicated prosecutor for confiscation, and asset tracers who examine the seizure/confiscation dimension in each case presented to the OM. In addition, LEAs can rely on the support of a specialised confiscation team (Team Criminal Cash Flows), coordinated by the LCA. The Team consists of a policy advisor and approximately 70 staff, including forensic accountants, civil law advisers, international legal advisers, asset tracers, public prosecutors and legal staff specialised in confiscation procedures. Upon request from all OM branches and LEAs in the Netherlands, the LCA can deploy the Team to provide support on complex confiscation cases, or lead confiscation proceedings. As noted under IO.1, with the setting-up of the MIT[37], the authorities are also increasingly targeting subversive crime, including from a confiscation perspective.

201. At an operational level, all LEAs set annual seizure targets to practically implement the instruction and priority assigned to confiscation. These targets have been increasing over the years, and have been generally met by all LEAs. The seizure target for special investigative services (BODs) is EUR 91.6 million a year in 2021 and 2022, of which EUR 70.4 million euros is accounted to the FIOD. The Police Central Unit has a target of EUR 25 million for 2021-2022, while the regional units have a confiscation target set at EUR 155 million. Police representatives met during the onsite indicated that they had already seized approximately EUR 15 million, as of October 2021.

Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

202. The Netherlands has a robust and comprehensive regime to deprive criminals of their assets through object and value confiscations. The authorities can apply two different conviction-based[38] confiscation schemes. Ordinary object confiscation is a penal sanction applicable when a defendant is convicted of any criminal offense, with respect to the proceeds directly obtained from the crime and instruments used to commit the crime.

[37] As of 1 July 2022, the MIT changed its name to NSOC. See also Box 2.1 in IO.1.

[38] The authorities are currently discussing the introduction of a legislative proposal for non-conviction based confiscation, to broaden their capacities to purse confiscation of criminal proceeds.

203. In addition, Dutch legislation provides for a special claim for value confiscation. Upon request of the OM, the court may issue a separate order for special confiscation consisting of the obligation for the offender to pay a sum of money to the State or to the victim in restitution of the illicit earnings, profits or advantages, as a fine or as a compensation for the victim. Upon conviction for an offence, the confiscation order may also be imposed for other offenses for which there are sufficient indications against the convicted individual. The confiscation order can be executed on all possessions of a convicted individual, regardless of their legal or illegal origins. Value confiscation proceedings can take place simultaneously with the main criminal proceeding, or after the criminal conviction has been obtained, as long as the application is lodged with the Court within two years after the first verdict. A particular strength of the Dutch legal framework is that, whenever a person is convicted of a serious and potentially lucrative crime, all income or assets obtained within six years prior to the conviction are deemed to be originated from, or connected to, the offence and can therefore be subject to confiscation. In such cases, there is a reversal of the burden of proof and it is up to the convicted to demonstrate the licit origin of such assets.

204. The OM has a high degree of discretion in deciding how to proceed with seizure or confiscation measures. Prosecutors may also choose to impose sanctions that have a similar effect, such as demanding compensation as part of an out-of-court settlement or imposing a penalty order. The high number of value confiscation procedures considered by the Court, or imposed by the OM through settlements or penalty orders confirms the priority assigned by the authorities to depriving criminals of their proceeds (Table 3.19).

Table 3.19. Number of value confiscation proceedings (OM and Court)

	2016	2017	2018	2019	2020	2021*
N. of Court decisions on value confiscation	2280	2320	2210	1810	1150	423
granted	1020	1010	970	790	490	135
partly granted	620	620	680	590	390	142
Value confiscation settlements	199	216	171	262	85	39
Penalty orders	140	111	66	51	11	46

* Covers the first half of the year.

205. Financial investigations are a crucial element for the authorities to obtain insight into the assets and flows of money associated with lucrative crimes. As noted under IO.7, LEAs dispose of a wide range of investigative tools, either within the regular investigation process, or within a criminal financial investigation, to detect criminal proceeds. iCOV data intelligence reports are also regularly used to obtain a comprehensive view on a suspect's financial position. This information is particularly useful to determine the amount of illegal profits or advantages obtained by the suspect, and to substantiate a value confiscation measure. LEAs and the OM dispose of a high-level of expertise to track criminal proceeds, as a result of specialised officers such as asset tracers.

206. LEAs make extensive use of seizures as a precautionary measure to ensure final confiscation. The OM can directly authorise most seizures, without the need for a court authorisation, as long as the seizure is based on an existing criminal investigation and there is a direct or indirect link between the object and the offence. Under the instruction of the OM, investigative officers can seize objects and assets, such as money, bank and savings accounts, jewellery, telephones, documents, vehicles and vessels, which constitute evidence or demonstrate the illegal nature of the proceeds.

207. In cases of serious offences, the authorities frequently use a prejudgment seizure to secure the right of recovery in connection with a monetary fine or confiscation measure to be imposed, or a compensation measure for the victims of crime, at an early stage of the investigation. In such cases, LEAs need a separate general authorisation (i.e., without specification of the objects to be seized) from the examining magistrate and in this context, they can also seize objects unrelated to the offence. The case below represents an example of the use of a prejudgment seizure.

Box 3.13. Use of a prejudgement seizure to preserve the right of recovery

The investigation related to large-scale drug trafficking and ML via VAs. In the course of searches in different premises, the Police found 85 kilograms of amphetamines and 13 kilograms of ecstasy pills. The suspects were dispatching drug orders received through the darkweb through postal services and were receiving payments in VAs. Upon authorisation from the examining magistrate, LEAs carried out a prejudgement seizure on three suspects, for a total amount of EUR 18 130 in cash, and 1.7 bitcoin. In 2020, the Court convicted four suspects to seven years' imprisonment for ML and drug trafficking. VAs, cars and approximately EUR 11 650 in cash were confiscated. The rest of the seized amount was kept under the prejudgement seizure for the value confiscation procedure that will follow.

208. The Assessment Team received limited statistics on the seizure and confiscation results obtained by the Netherlands. However, a review of the case studies and information provided by the authorities on the registration of the seizures by predicate offences demonstrate a correlation between the value of the seizures and the main proceeds generating crimes (ML, drugs-related crimes, fraud and organised crime).

209. The Dutch authorities provided an overall number of seized assets between 2016 and 2021, which is presented in Table 3.20 below. However, the authorities also acknowledged that the numbers are incomplete, in particular in relation to the value of outgoing seizure requests to foreign countries, and of seizures in the Netherlands based on a MLA request. Information on the number of European freezing orders sent and received by the Netherlands is available under IO.2; however, it was not possible to determine the overall number of cases where a seizure was obtained.

Table 3.20. Value of seized assets (million EUR)

	2016	2017	2018	2019	2020	2021*
Total	431.4	570.8	502.9	329.5	403.5	256.2
Seizures by BODs	106.2	294.4	253.0	106.5	123.5	135.1
Seizures by Police	318.2	271.3	239.1	215.3	266.0	117.5
Seizures by other LEAs (e.g., KMar, Customs)	7	5.1	10.8	7.7	14	3.6

* Covers the first half of the year

210. The Netherlands has an effective system to manage and preserve the value of seized assets (deriving from both domestic and international seizures), through an appropriate registration mechanism and sufficient facilities to store seized and confiscated goods. DRZ, an agency of the Ministry of Finance, manages seized and confiscated goods. The OM, advised by its the National Authority for Seized Goods (LBA), decides what should happen to seized assets, in order to preserve their value: whether to return, retain, deposit, sell or destroy them. Between 2016 and 2020, DRZ processed more than 27 034 items and obtained approximately EUR 35.9 million from sold goods. Table 3.21 details the actions undertaken by the DRZ in relation to prejudgement seizures.

Table 3.21. Objects received and processed by DRZ for prejudgement seizure

	2016		2017	2018	2019	2020
Objects received by DRZ (number)	4979		6814	6875	4425	3941
	Objects managed by DRZ					
- Returned (number)	2236		2557	3150	2397	2708
- Sold (number)	2029		2148	2114	2714	1829
- Destroyed (number)	221		393	314	424	253
Value of sold goods (EUR)	6.9 M		7.1 M	6.7 M	7.3 M	7.9 M

Note: An object number does not indicate the volume or number of articles it contains. For example: one object may actually consist of several pieces of jewellery. The value of sold goods is already included in the overall seizure results under Table 3.20.

211. The authorities have also pursued the tracing of VAs related to criminal activities and successfully seized an increased number of assets over the last few years (see Box 3.15). This is demonstrated by case studies provided by the authorities, as well as by the statistics on VA seizures presented in Table 3.22 below.

Table 3.22. Annual seizure of VAs

	2019	2020	2021*
Value of seized VAs in EUR	1.1 M	8.3 M	34.6 M

* Covers the period up to 18 November.
Note: The value of seized VAs is already included in the overall seizure results under Table 3.19.

Box 3.14. Process for tracing and seizing VAs

Tracing and seizing VAs has become a national priority since 2017. LEAs developed specialised expertise and set-up specialised teams to trace VAs, by de-anonymising the VA trail. The OM can authorise the seizure of any object, including VAs. If the wallet is located in the Netherlands, LEAs are authorised to conduct a search. If the wallet is located abroad, the authorities would proceed with a MLA request, either judicial or police-police, or other type of international co-operation as appropriate. Where a VA exchange is not located in any particular jurisdiction, the Netherlands can apply the Dutch law and proceed with a seizure or confiscation. As noted under IO.7 (Box 3.9), the Netherlands has also demonstrated its ability to seize mixing services, by seizing the servers.

Once VAs are seized, they are stored in an OM wallet at the Dutch exchange. To avoid the volatility associated with the value of VAs, as a policy the Netherlands sells the seized bitcoins in exchange for EUR, as soon as it is reasonably practical.

212. In Netherlands, the OM uses multiple paths to deprive criminals of their assets, through object and value confiscation. A case example of the use of object and value confiscation is presented in Box 3.16 below. The OM frequently reverts to out-of-court settlements in order to seek compensation. Out-of-court settlements include a wide range of measures, depending on the single case, and often comprise confiscation orders, and fines. The Netherlands does not have separate confiscation statistics for proceeds deprived pursuant to a conviction-based confiscation, and a non-trial solution through an out-of-court settlement. Separate statistics on out-of-court settlement confiscations are maintained only for multi-million Euro cases against legal persons (Table 3.24). The execution of confiscation is the responsibility of the Central Judicial Collection Agency (CJIB), which is the authority in charge of the collection of fines and the handling of decisions under criminal law.

Box 3.15. Use of different forms of confiscation in a ML case

An individual on disability benefit, with no other income, deposited large amounts of cash into his bank accounts for over EUR 270 000 during several years. The investigation revealed he had deposited over EUR 12 million into other bank accounts and then transferred the money to companies and foreign bank accounts. False documents were used to cover-up the transactions, which were not related to any business activity. The suspect was using strawmen to hide that the companies were actually under his control. He was arrested at Schiphol airport, carrying over EUR 40 000 in undeclared cash. He was convicted to 65 months of prison for habitual ML, as he was unable to provide any reasonable explanation on the origin of the money. The court ordered the object confiscation of more than EUR 550 000. Furthermore, in a separate value confiscation procedure, a payment of over EUR 340 000 was also imposed, to recover the suspect's illegally obtained gains. As a result of this investigation, the Agency for disability benefit also initiated a recovery procedure for over EUR 65 000. Other convictions and confiscation measures were imposed on his accomplices.

3

213. Overall, the Netherlands achieved a collected confiscation value of over EUR 399 million in the period between 2016 and the first half of 2021, as a result of confiscation imposed both after conviction, and as part of out of court settlements (Table 3.23). In addition, the Dutch authorities have confiscated large amounts through multi-million out of court settlements in some high-profile cases related, for instance, to non-compliance in the banking sector or major corruption cases against legal persons. The confiscation component of the settlement is considerable, with a total amount of EUR 967.3 million since 2016, as shown in Table 3.24 below.

214. The Assessment Team notes that these major out of court settlements account for a large part of the overall confiscation results. These values refer exclusively to the collected assets, as opposed to the value of confiscation orders imposed by the Courts which is higher.[39] There is also a discrepancy between the year of the initial seizure and the year of the final collected confiscation, as the confiscation process may take several years.

Table 3.23. Value of collected confiscated assets (million EUR)

	2016	2017	2018	2019	2020	2021*
Confiscated assets in EUR million	72.7	76.3	71.3	78.2	84.7	16.1

* Covers the first half of the year.

Table 3.24. Confiscation amounts in major out of court settlements with legal persons (million EUR)

	2016	2017	2018	2019	2020	2021*
Confiscation value	329.3	144.9	100	183.6	n/a	209.5

* Covers the first half of the year.

215. Furthermore, the authorities provided statistics on the number of confiscation decisions achieved in cases where a ML conviction (both as stand-alone and in mixed cases) was imposed (Table 3.25). This data, considered with the annual number of value confiscation proceedings by the Court, and settlements by the OM supports the conclusion that the authorities are focusing on confiscating criminal proceeds.

39 The Netherlands does not collect statistics on the value of confiscation orders imposed by the Courts.

3

Table 3.25. Number of imposed Court confiscation decisions in mixed and stand-alone ML convictions

	2016	2017	2018	2019	2020	2021*	Total
Confiscation orders on natural persons	93	118	156	204	154	190	915
Confiscation orders on legal persons	8	1	3	2	5	13	32

* Covers the first half of the year.

216. The Netherlands has a solid structure to cooperate internationally on asset recovery matters. The Asset Recovery Office (ARO) acts as special contact point for asset confiscation and received a total of 578 incoming and outgoing requests related to asset freezing and confiscation in 2020 (see IO.2). The Asset Management Office (AMO), within LBA, handles seizures made in the Netherlands pursuant to a foreign authority request or freezing order and engages with the foreign authorities to discuss the proposed approach to maximise yields. In the event of an international seizure, the requesting country will eventually transfer the execution of the underlying case to the Netherlands, after which the verdict can be enforced by the CJIB using the seized assets. In this execution phase, the competent authorities of the states involved can make agreements about asset sharing.

217. The authorities did not provide specific information on asset sharing and recovery of proceeds involving foreign predicate offences, or proceeds moved to other countries, with the exception of the amounts confiscated through European confiscation orders (see IO.2). The values of the confiscation orders sent by the Netherlands is noteworthy: approximately EUR 38.9 million between 2017 and 2020.[40] The cases presented by the authorities showed a strong and effective co-operation with international counterparts to trace and seize criminal assets. The case below is an example of successful asset-sharing with Spain.

[40] This amount is already included in the confiscation results in Table 3.23.

Box 3.16. Example of successful asset-sharing

In November 2020, the OM issued a penalty order against an individual, due to his failure to pay an outstanding amount of EUR 339 million, imposed in a value confiscation procedure. The convicted person flew to Spain, where he was arrested based on a Belgian European Arrest Warrant. In May 2021, the Dutch liaison officer to Spain contacted the CJIB, and further to the co-operation with the Spanish authorities and an ARO request, the valuable objects found during the arrest were seized. A few days later, CJIB sent a confiscation order to Spain (based on EU Regulation 2018/1805). In August 2021, CJIB received a confirmation that the seized objects (two cars, two scooters and a water scooter) would be sold and the proceeds would be shared 50-50 between the Netherlands and Spain. The Netherlands received EUR 30 500.

218. Prosecutors also pursue victim compensation (restitution) as part of the criminal or confiscation case. If the suspect/convict possesses illegally obtained gains and an injured third party exists, the OM Confiscation Instruction directs prosecutors to issue a demand for a confiscation order. The Netherlands has provided some examples (see Box 3.18), but no statistics are collected on the overall number of cases or amounts returned to victims, as the corresponding value are not included in the collected confiscation results (Table 3.23).

Box 3.17. Example of victims' restitution

LEAs conducted an investigation into a network of criminals exploiting women from Eastern Europe for prostitution. EUROJUST was involved, and a joint investigative team with Hungary was created to identify the criminal network. The investigation was conducted between 2014 and 2015. In the course of the investigation, the ARO seized several assets of the suspects, including real estate, two cars, and bank accounts. In 2016, the main suspects were convicted of human trafficking and ordered to pay compensation to their victims for a total of EUR 459 000.

219. Finally, the authorities also rely on tax and administrative measures as a complementary tool to recover criminal assets, by levying taxes, imposing tax fines or seizing wages or benefits. An example of this integrated approach is presented in Box 3.19.

Box 3.18. Use of tax measures in addition to confiscation

An individual was convicted to 12 years' imprisonment for ML, international drug trafficking and possession of firearms. Criminal assets valued over EUR 3 million were seized and confiscated under criminal law. Value confiscation proceedings regarding illegally obtained gains (over EUR 15 million) were still awaiting decision in second instance at the time of the onsite visit. In addition to these criminal confiscation measures, the Tax and Customs Administration seized a luxury car under tax law, and a report was submitted to the municipality in order to recover undue social benefits provided to the convict and his wife.

220. In the BES Islands, there are limited statistics available on the level of seizures and confiscations. Between 2017 and 2020, a total of 12 cases involved confiscation. The annual confiscation target of USD 20 000 was largely exceeded in the years for which statistics are available. For instance, the overall value of confiscated assets was USD 315 500 in 2017, USD 76 500 in 2018 and USD 331 000 in 2019. However, the authorities have also established an annual target in terms of number of confiscation proceedings per year (two), which was not achieved in 2018 and 2020.[41]

221. The Assessment Team is unable to provide a clear interpretation of these figures. However, the limitations noted under IO.7, in relation to the ability of LEAs in the BES to perform financial investigations, also affect the confiscation results and therefore the Assessment Team welcomes the recent increase in resources and training for BES OM and LEAs. The annual value of confiscated assets suggests a need to review the annual target of USD 20 000.

Confiscation of falsely or undeclared cross-border transportation of currency/BNI

222. The Dutch authorities are aware of the risks related to the cross-border transportation of cash and valuable goods associated with criminal activities and demonstrated an ability to seize assets at the borders, in particular at high risks ports of entry, such as the Schiphol international airport.

223. Several LEAs are involved in investigating cross-border movements of cash, including Customs, KMar, FIOD, and cooperate closely with the district prosecutors. Custom officers are designated as special investigative officers and can apply criminal investigative powers when performing their tasks (see R.31). The low threshold for a suspicion of ML enables them to easily initiate a criminal investigation whenever the origin of money is unclear, or undeclared cash or BNIs are found. In the performance of its tasks, Customs uses some risk-indicators, mainly based on FEC studies, NRA results, signals received, with the main one being the country of origin or destination of the passenger, based on a list of countries identified as high-risk.

[41] During the onsite visit, the authorities also noted that OM BES was preparing a confiscation proceeding for approximately USD 6 million, in relation to a major drug trafficking case.

224. Most undeclared cash or money courier cases detected by Customs or KMar occur at Schiphol Airport. The Netherlands has therefore set-up a specialised investigation team at Schiphol where KMar and FIOD work together, under the lead of a dedicated team of prosecutors from the Noord-Holland OM office. All suspicions of ML identified by Customs are transferred to this team. In the BES Islands, Customs Caribbean Netherlands and KMar perform AML/CFT tasks at the borders, in co-operation with the OM BES.

225. Customs, including in the BES Islands, makes all cash declarations and disclosures available to FIU-NL within four days through goAML. As noted under IO.6, this information becomes part of the FIU-NL UTR database. Table 3.26 shows the overall number and value of cash declarations and disclosures. These figures include both the declarations over the threshold received by Customs, and the number of reports for violation of the obligation to declare.

Table 3.26. Number and value of cash declaration/disclosure reports (extra-EU and BES Islands)

	2016	2017	2018	2019	2020	2021*
Sea	1475	1097	1428	1412	1778	1492
Air	3311	3280	3247	3121	3242	1651
BES Islands		46	57	38	95	
Total reports	4 786	4 423	4 732	4 571	5 115	3 143
Value NL in EUR	284. 5 M	201.3 M	171.4 M	199.1 M	268.5 M	184.4M
Value BES Islands in USD	4.5 M	4.5 M	4.2 M	14.2 M	20 M	7.6 M

* Covers the first half of the year.

226. As of June 2021, the Netherlands has started implementing the new EU regulation 2018/1672, which imposes a disclosure obligation for the transportation of cash/BNI via cargo. The implementation of this new regulation is too recent to assess in terms of effectiveness. The Netherlands implements a broad disclosure system for intra-EU transportation of cash and valuable goods, pursuant to their national customs regulation. The so-called "right to report" allows Customs to request passengers travelling within the EU to disclose information on cash or other types of valuable goods. Table 3.27 below provides an overview on the number of disclosures and the type of related valuable goods. These intra-EU disclosures led to over 50% of the ML investigations initiated by Customs between 2016 and June 2021.

Table 3.27. Number and value of intra-EU disclosures (million EUR)

	Number	Amount (M EUR)	Number	Amount (M EUR)	Number	Amount (M EUR)	Number	Amount (M EUR)	Number	Amount (M EUR)
	2016		2017		2018		2019		2020	
Total	334	102.3 M	391	119.6 M	351	40.5 M	253	25.2 M	192	24.8 M
Of which, main figures relate to:										
Watches	69	30.3	86	9	145	16.6	92	10.4	63	5.3
Gold	111	13.2	121	76	41	5.7	20	3.2	15	2.3
Precious stones	20	34.2	18	17.8	11	3.7	6	0.8	2	6.8
Jewellery	39	5.6	31	7.1	36	7.2	24	5.7	11	4.1
Intra EU cash	69	2.5	93	2.6	90	2.4	87	3.1	78	2
Other	26	16.5	42	7.1	28	4.9	24	2	23	4.3

227. The Netherlands pays particular attention to the use of valuable goods to transfer criminal profits from, and into, the country. During the onsite visit, the authorities presented cases to the Assessment Team where individuals were caught travelling with very expensive watches and could not provide a satisfactory explanation on their origin. In such cases, Customs initiated a ML investigation and submitted a UTR to the FIU-NL. In a recent case, the Customs report was picked-up by the FIU's queries system, and after in-depth analysis by FIU analysts, and crosschecking of information with iCOV, JustisTRACK and two FIs, FIU-NL disseminated it to LEAs for further investigation.

228. Overall, Customs initiated a reasonable number of ML investigations based on violations of the obligation to declare or the obligation to disclose, as shown in Table 3.28. Customs seized assets for over EUR 22.7 million. Box 3.20 provides a case study on a ML investigation initiated by Customs.

Table 3.28. Investigations initiated by Customs

	2016	2017	2018	2019	2020	2021*
Extra-EU declarations	36	23	32	37	33	23
Asset seized (EUR)	3 M	1.33 M	2.09 M	2.95 M	1.84 M	2.12 M
Intra-EU disclosures	17	31	43	38	51	25
Asset seized (EUR)	0.85 M	0.89 M	1.58 M	2.06 M	3.20 M	0.79 M
Total ML investigations	53	54	75	75	84	48
Total seized assets (EUR)	3.85 M	2.2 M	3.6 M	5 M	5 M	2.9 M

* Covers the first half of the year.

229. The authorities did not provide statistics on the follow-up to these cases, which limits the ability of the Assessment Team to fully assess Customs' contribution to depriving criminals of their assets. In the BES Islands, between 2015 and 2020, Customs transferred eight investigations to other LEAs, following a violation of the obligation to declare and a suspicion of ML. Out of these cases, only one led to the arrest of the suspect. The others were either dismissed by the OM, or closed with a fine or a settlement.

3

Box 3.19. ML investigation initiated by Customs

In 2019, Customs at Schiphol airport discovered over EUR 1.38 million in cash in the suitcases of an Italian resident intending to travel to China via Amsterdam. The suspect was arrested on the suspicion of ML and the deliberate failure to declare the money to Customs. The suspect ultimately admitted he was transporting undeclared cash. The FIOD conducted an investigation into the origin of the money but could not determine the predicate offence, except for the suspect's statement that he partly did not pay taxes. A recorded conversation while the suspect was in custody also indicated tax evasion and revealed that the money belonged to the defendant himself. The Court concluded that the suspect did not provide any substantiation for the legal origin of the money. He was sentenced to 30 months' imprisonment for ML, and the money was confiscated.

230. In addition to the cases that resulted in the opening of a ML investigation, Customs have also applied fines for failure to declare. However, as noted under R.32, the Assessment Team considers that the maximum level of fines, corresponding to a third or fourth category fine (EUR 8 700 or EUR 21 750) is not proportionate or dissuasive. The low level of penalties applied in practice also impacts their dissuasiveness (see Table 3.29). The same conclusions extend to the BES Islands.

Table 3.29. Penalties applied for violation in the obligation to declare

	2016	2017	2018	2019	2020	2021*
Customs Netherlands						
Number of total violations	398	1249	1054	1143	624	308
Number of violations for which a penalty is applied	349	968	920	965	460	285
Total penalties (EUR) (average in EUR)	344 800 (988)	718 600 (742)	603 200 (656)	814 700 (844)	543 000 (1 180)	403 233 (1 415)
Customs BES						
Number of total violations	2	0	4	8	2	3
Number of violations for which a penalty is applied	0	0	0	5	2	3
Total penalties (USD) (average in USD)	0	0	0	10 152 (2 030)	1470 (735)	4 491 (1 497)

* Covers the first half of the year.

Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

231. Available statistics and case studies provided confirm the authorities' focus on the confiscation of criminal assets, in line with national policies and priorities. The limited statistics available do not provide a comprehensive picture of the authorities' results in this respect. However, they are sufficient to establish a correlation between the seizure results obtained by the Netherlands, and the prevailing proceeds-generating offences in the country.

232. In the BES Islands, authorities have achieved some results in confiscating criminal proceeds. However, in the absence of more detailed information, it is unclear whether these results are consistent with ML risks.

Overall conclusion on IO.8

The tracing and confiscation of criminal assets is a clear priority for LEAs and the OM. The strong legal measures available, and the specific financial expertise enable LEAs to conduct complex criminal investigations and trace proceeds of crime. A large proportion of the confiscation results is linked to major out of court settlements imposed on legal persons. Although comprehensive and detailed statistics are not available, confiscation results are in line with national policies and the national risk profile. The collected confiscation results do not reflect the overall value of confiscation orders imposed by the Courts.

The Netherlands has achieved good results in seizing cash and valuable goods at the borders, and initiating subsequent ML investigations. However, the level of sentencing applied for the violation of the obligations to declare is low, which impacts its dissuasiveness.

The Netherlands is rated as having a substantial level of effectiveness for IO.8.

Chapter 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

1. The Netherlands has a robust framework to detect, investigate and prosecute TF. The Netherlands is able to detect signals from many different sources and to launch TF investigations, both in parallel to terrorism investigations, and autonomously. The effective co-ordination in place between all relevant stakeholders involved in countering TF, such as the Programme FEC-TF, is a strength. The FIU-NL, in particular, has significantly contributed to TF investigations, 50% of which were triggered by its disseminations. The Table of Four, under the OM, ensures that all signals are considered and TF cases prioritised.
2. The types of TF investigated and prosecuted are in line with the country's risks, with a high majority of cases involving the funding to FTFs. While some investigations of NPOs possibly involved in TF are ongoing, no conviction has been achieved so far, which is not in line with the high risk associated to the abuse of NPOs in the TF NRA. The authorities are also monitoring possible new and emerging TF threats, such as right-wing terrorism. No TF case has been detected in the BES Islands to date, which is consistent with its TF risk profile.
3. The conviction rate in TF cases is high (70%). Nevertheless, the level of TF sentencing imposed in practice is generally low, which affects the dissuasiveness of the sanctions. There are no TF guidelines for the prosecution or sentencing orientation points for judges. While the prosecution policy is that a prison sentence should be requested in all TF cases, almost half of the judgements resulted in a community service or a suspended prison sentence.
4. The Netherlands uses a wide range of alternative measures where it was not practicable to obtain a TF conviction, including pursuing other criminal charges, or adopting administrative measures, such as halting social benefits, revoking citizenship or imposing travel bans.

Immediate Outcome 10

1. The Netherlands implements UN designations without delay, through a combination of EU and national provisions. It has made proactive use of domestic designations to target FTFs, in line with its risk profile. The obligation to freeze assets and the prohibition on making funds available

apply to all persons, including all obliged entities. Nevertheless, in practice, the lack of supervision of the implementation of TFS without delay_for DNFBPs other than trust offices, and VASPs and certain DNFBPs in the BES Islands, creates a potential gap in the implementation of TFS without delay.

2. There are tools to communicate changes to the sanctions lists. For UN and EU designations, the Netherlands relies mainly on the publication of the changes on the UN website and the EU Official Journal. Domestic designations are published on government websites and the Official Gazette. DNB and AFM disseminates changes to the national and EU lists in their monthly newsletters. However, some of these communication channels are available only to subscribers and may not always ensure the timely communication of new designations.

3. The Netherlands has a robust understanding of the TF risks associated with the abuse of NPOs. It has also identified the characteristics of organisations at higher risk of TF abuse, even if the authorities have some difficulties in identifying all the organisations that correspond to this profile, as some charitable foundations operates without an ANBI status of CBF seal.

4. Self-regulation is a key feature of the Dutch non-profit sector. The Netherlands has no supervisory authority to monitor NPOs. Voluntary certification mechanisms, such as the ANBI status and CBF seal, promote transparency and accountability among participating NPOs. The authorities undertake extensive outreach to the categories of "good faith" NPOs, which, by virtue of their activities, present a higher risk of potential TF abuse and have jointly developed good practices to raise awareness on TF risks and vulnerabilities. The sample of organisations met by the Assessment Team were well aware of their TF risks. Good faith NPOs, including those at higher risk, are already implementing effective TF risk mitigation measures and are engaged in regular dialogue with the authorities.

5. Authorities use financial, administrative and criminal and intelligence information to detect NPOs sponsoring terrorism. However, due to the limited visibility on the activities of some NPOs and the lack of any legal requirement on transparency and accountability, it is difficult to collect sufficient evidence to start an investigation or to designate them for TFS. Furthermore, until a criminal conviction is achieved, so-called "bad faith" NPOs can continue operating, raising and moving funds.

6. The amount of funds frozen based on domestic designations is overall low, which is consistent with the country's TF risks. The Netherlands has confiscated a very limited amount of TF-related assets, due to challenges in seizing money in conflict zones and in collecting sufficient evidence to investigate charities possibly involved in supporting terrorism.

Immediate Outcome 11

1. The Netherlands (including the BES Islands) implements UN designations without delay, through a combination of EU and national provisions. The mechanism in place to implement PF-related TFS is identical to the one for TF designations and the freezing obligations apply to any person, including all obliged entities. However, as the implementation of TFS without delay

by DNFBPs, with the exception of trust offices is not supervised, the assessment team has doubts about their ability to implement TFS without delay. The same considerations noted in IO.10, in relation to communication mechanisms apply to PF TFS.

2. In total, between 2016 and 2021 the Netherlands identified 15 matches with PF-listed persons/entities. In seven cases, funds were frozen. With the exception of a major freezing and other minor ones by a branch of a Dutch bank located in Asia in relation to DPRK sanctions, the Netherlands has frozen only a few hundred EUR in relation to Iranian PF sanctions. These figures are consistent with the Netherlands' low exposure to PF. However, as there is no explicit obligation for DNFBPs to report assets frozen or action taken to implement TFS, and there is no supervision on their implementation of TFS obligations, the authorities may have only a partial view of the implementation of TFS implementation by these entities.

3. The authorities have identified some violations related to sanctions obligations, in particular in relation to the export of dual use, or luxury goods to DPRK. The supervisors or the OM Office investigated all detected breaches and the authorities prevented the goods from reaching their final destination. Nevertheless, as there is no supervision of the implementation of TFS without delay for DNFBPs except trust offices, and their supervisors do not perform specific controls regarding TFS, sanction breaches involving DNFBPs are less likely to be identified.

4. The understanding of TFS obligations is strong in the financial sector. DNB and AFM have provided guidance on sanctions implementation to FIs and trust offices and have followed-up on identified breaches to ensure the adoption of remedial actions. These actions generally resulted in increased compliance. DNFBPs met during the onsite visit had a good understanding of their TFS obligations, and most were performing checks against the UN and EU sanctions lists. However, in the absence of any supervision, it is unclear whether the entire DNFBP sector, and DNFBPs and VASPs in the BES Islands, are implementing TFS obligations at a satisfactory level.

Recommended Actions

Immediate Outcome 9

1. The Netherlands should review the current level of sanctions applied in TF cases, to ensure that they are dissuasive and consider developing specific TF guidelines for the OM and sentencing orientation points for judges.

2. The Netherlands should continue its efforts to develop a broad range of financial intelligence to identify and pursue TF cases, including those related to the use of unlicensed payment services and NPOs, and adopt effective enforcement action.

3. In the BES Islands, the authorities should use all intelligence leads, including financial intelligence, to detect any possible signal of TF.

Immediate Outcome 10

1. The Netherlands should consider clarifying the criteria for proposing designations to the UN 1267 Committee, the EU COMET and third countries, to ensure they are properly understood and implemented by the authorities.
2. The Netherlands should further improve communication to ensure that legal and natural persons, and obliged entities in particular, are notified promptly of any change in designations, including at the UN level.
3. The Netherlands should conduct a comprehensive NPO TF risk assessment, to better identify those organisations most vulnerable to potential TF abuse, in particular amongst those operating without ANBI or CBF certifications and, on this basis, assess the effectiveness of existing mitigating measures and implement targeted controls and risk-based transparency requirements on non-certified NPOs posing a high-risk of TF abuse.
4. The Netherlands should take measures to ensure that all charitable organisations, including church communities, are identifiable.
5. The Netherlands should continue pursuing its proactive engagement with NPOs and the private sector, to avoid de-risking and facilitate NPO's access to financial services.
6. The Netherlands should enhance the financial transparency of NPOs and the donations they receive, including by passing and implementing the proposed law on transparency for civil society (WTMO).

Immediate outcome 11

1. The Netherlands (including BES Islands) should require all categories of obliged entities, to take adequate measures to implement TFS without delay, report frozen assets and any action taken pursuant to TFS obligations.
2. The Netherlands (including BES Islands) should ensure that the implementation of PF TFS by all obliged entities is monitored by supervisors.
3. The Netherlands should maintain statistics to assess whether obliged entities adequately freeze and report frozen funds or assets from designated individual or entity without delay.

233. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

234. The Netherlands has a strong understanding of its TF risks, informed by the two TF NRAs, terrorism threat assessments, and by the thematic investigation projects carried out by the authorities (see Project A and Project T below). As noted under IO.1, religious terrorism poses the most significant threat to the Netherlands, in the form of Dutch FTFs who travelled to conflict zones to join terrorist groups, and domestically in the form of radicalised individuals, abroad or in the country, attempting to spread extremist ideologies in local communities. The Netherlands is also closely monitoring new emerging terrorist threats, such as right-wing terrorism. The 2019 TF NRA identifies the following channels and methods as posing the main TF risks:

- foundations and other legal entities both in the Netherlands and abroad;
- legally acquired funds; and
- licensed and unlicensed payment services.

235. For BES Islands, the ML/TF NRAs did not reveal any clear signals of TF threats and the Dutch authorities therefore infer the TF risk as low.

236. In recent years, the Netherlands has experienced a number of terrorist incidents and thwarted plots, mostly carried out by lone actors. While most of these were related to religious terrorism, there have also been incidents involving right-wing terrorism. As of April 2021, approximately 105 out of the 305 FTFs who had travelled from the Netherlands were still in Syria and Iraq.

237. The majority of TF cases investigated until November 2021 involve the provision of financial and material support to FTFs, which is in line with the Netherlands' risk profile. The Netherlands prosecuted 27 TF cases between 2016 and 2020. In 19 cases, a TF conviction was achieved, while eight were acquitted, or are currently pending trial or in appeal. The different types of TF cases prosecuted and convicted involves raising funds through legal and illegal means. Licensed and unlicensed payment services feature as the main channels used to transfer funds. While some ongoing TF investigations involve the possible abuse of NPOs for TF purposes, no conviction has been achieved so far, which is not in line with the high risk associated to the abuse of NPOs in the NRA. Box 4.1 provides some examples of the sources of TF used in the investigated cases.

Box 4.1. Case examples on the financing of FTFs

Use of legal funds

In 2019, an individual was convicted of TF and violations of the Sanctions Act for transferring EUR 200 via a money transfer service to an intermediary in Turkey in 2014. The money was sent to a family member participating in ISIL in Syria. The Court imposed a sentence of two months' imprisonment with a probationary period of two years.

4

Financing through the abuse of NPOs

Upon proactive analysis, the FIU-NL identified an NPO active in charitable projects in Syria and Iraq, linked to high-risk transactions related to ML/TF. The NPO was also in direct contact with suspected terrorist sympathisers in Netherlands and Belgium. The FIU-NL detected money flows to a NPO in Turkey, which was an intermediary to re-direct money and goods to Syria. The Court proceeding is ongoing.

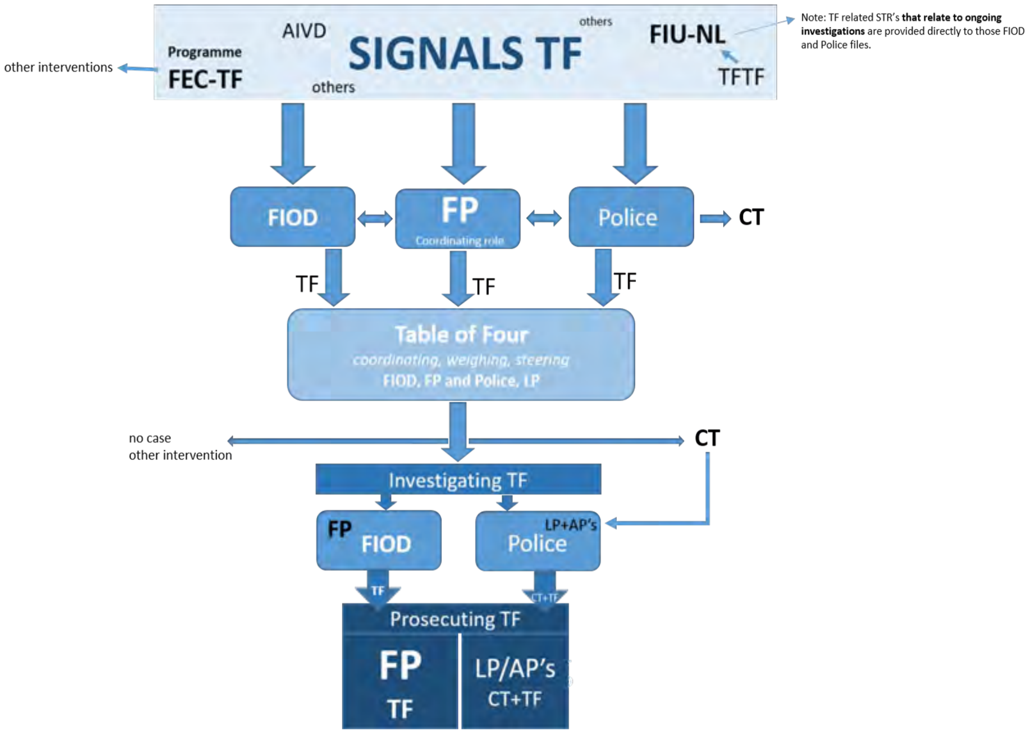
Use of unlicensed payment services

In 2020, an individual was convicted of TF, illegal banking and human smuggling. Between 2016 and 2018, the individual knowingly transferred money via hawala channels to family members fighting for ISIL. The case came to light upon a domestic violence report made by his ex-wife, who disclosed the hawala channels used by the individual to record payment orders to operators and deliver the money to Syria and Turkey. The Court imposed a sentence of 36-month imprisonment with a probationary period of one year (the charges included also other offences not related to TF).

238. The Dutch authorities, in particular the OM, FIOD, Police and FIU-NL, have accorded priority to CFT. TF cases have been assigned to a designated and secure court in Rotterdam, which hears the cases since early 2019 on a bi-monthly basis in order to absorb the prosecution caseload. As discussed with members of the judiciary during the onsite, the OM and courts assign priority to TF cases.

TF identification and investigation

239. The Netherlands has a robust institutional framework to proactively identify and assess any signal related to TF and coordinate the most appropriate response, from the intelligence phase to the investigation and prosecution. There is close co-operation and co-ordination between the authorities in charge of terrorism and TF investigations. The FIOD handles autonomous CFT investigations under the authority of the OM/FP. FIOD has a dedicated CFT Team with 25 investigators. The Police Central Unit (LE), under the authority of the OM/LP, generally manages CT investigations. Within the LE, eight staff work on CFT issues detected in the framework of ongoing terrorism investigations. The OM/FP coordinates both the intelligence (signals) and the criminal investigation phases. The below diagram outlines the role of the various authorities in TF investigations.



240. To date, there have been no TF signals or investigations in the BES Islands, which is in line with its TF risks. Should any TF signal be detected, the OM/FP would cooperate with the OM Carib to coordinate the investigation.

241. TF signals are reported and discussed at the Table of Four, an operational platform led by OM/FP, where the FP, LP, FIOD and NP discuss information and decide whether to initiate a TF criminal investigation. The Table of Four has a no prioritisation policy, whereby all TF intelligence brought to its attention is considered. This approach ensures that no information is left unexamined. The Table of Four assigns the investigation to FIOD or the Police. It can also decide to pursue an investigation into a different criminal offence, such as fraud or ML. Within the OM, as a standard policy, TF investigations are conducted centrally by the FP. Every OM unit that comes across a TF signal should report it to the FP for co-ordination.

4

242. TF cases are identified either in the framework of ongoing terrorism investigations, or in the course of autonomous TF investigations. The Dutch authorities make full use of all possible intelligence sources, including reports from the General Intelligence and Security Service (AIVD), FIU-NL, Police, FIOD, co-operation projects and information from foreign counterparts, to identify TF signals. Programme FEC-TF plays an important role at this stage. The authorities also make use of public-private partnerships such as the TF Platform and the TF Taskforce to obtain additional insights and improve the quality of TF-related financial intelligence (see Box 4.2 below).

Box 4.2. CFT partnerships

The **Programme FEC-TF** regroups 13 governmental organisations to analyse criminal, administrative and tax information with a view to countering TF and mapping the financial networks of persons and entities known to the FEC participants, or identified in FEC signals. The insights obtained lead to drawing up an intervention strategy, or sharing lessons learnt among the participants.

FEC TF Task Force is a public-private initiative established in 2017. The Task Force allows investigative service (Police/FIOD) to share concrete TF signals and personal data (specific operational information) with banks, giving them concrete information that enable them to perform their statutory Wwft duty and search their systems. UTRs identified by banks trigger FIU-NL's investigation and dissemination to LEAs. Such sharing of signals and reporting of unusual transactions takes place under strict legal conditions.

The **TF Platform** is a public-private initiative established in 2012, by the Dutch Banking Association and FIU-NL. The purpose of the Platform is to enhance the quality and effectiveness of UTRs reported on TF. Via this Platform, the FIU shares knowledge of themes, phenomena and typologies with the four Dutch major banks. In addition, research is conducted into the development of TF risk profiles.

243. The FIU-NL has so far contributed to a high number of TF investigations, through targeted TF intelligence and the use of data profiling to detect TF-related cases for dissemination, based on thematic projects, such as the Project T. It has also provided extensive guidance to obliged entities to enable them to detect TF-related transactions.

Box 4.3. Project T

In 2013, FIU-NL developed a specific TF risk profile to detect the financing of FTFs by aggregating data on individuals who travelled to Iraq and Syria as FTFs or settled in the ISIL area, with analysis carried out within the TF Platform and data from domestic, UN, EU and foreign sanctions lists. The FIU subsequently shared the risk profile with obliged entities. Since 2013, it has resulted in over 1 600 UTRs, of which over 70% were found suspicious and disseminated by the FIU to LEAs. The TF risk profile developed through this project is used to scan daily UTRs in the FIU database and has been adapted to reflect the evolving nature of the TF threat (e.g., to focus on hubs of returning FTFs).

244. The Dutch authorities have conducted a total of 59 TF investigations in the period between 2016 and November 2021, involving 99 natural and four legal persons. 73% of the TF investigations are related to FTFs and around 8% are related to NPOs. Investigations conducted by the police or FIOD make extensive use of datahubs such as iCOV and the CT Infobox to gather as much information as possible on the subjects in a timely manner (see IO.6 for more information on datahubs). A number of TF cases and projects also demonstrate the frequent deployment of special investigative techniques, including wiretapping and surveillance, and an early engagement with the foreign counterparts to identify terrorist financiers and their domestic and international networks.

Box 4.4. Project A

Project A, initiated by FIOD and OM/FP, is a series of ongoing investigations, started in 2015. The project stemmed from previous investigations into the role of an intermediary transferring money to FTFs. Authorities involved were the FIU-NL, FIOD, OM/FP, Police, CT Infobox, EUROJUST, EUROPOL, and investigation services from the US, Spain, France and Belgium.

An intermediary was involved in several money transactions to FTFs from the Netherlands and several countries in Western Europe and North America. On the initiative of the OM/FP, these countries were informed via a EUROJUST meeting. The Dutch investigations focused on identifying the Dutch individuals who were ultimately providing financial support to FTFs. Subsequently, the project went on with the co-operation amongst foreign authorities in order to gain insight into the middleman and other intermediaries, with a view to identify and prosecute them.

TF investigation integrated with –and supportive of- national strategies

245. TF investigations are integrated in, and supportive of, the Netherlands overall CT policy and strategy. TF is explicitly embedded in the National Counterterrorism Strategy 2016-2020. The Strategy outlines an integrated approach to countering all forms of extremism and terrorism through five intervention areas: procure, prevent, protect, prepare and pursue. The TF component is particularly relevant in the areas of procuring (e.g., gathering financial intelligence on TF, financial networks and financial transactions), preventing (e.g., disrupting access to means and financial resources necessary to conduct an attack) and pursuing (e.g., investigating and prosecuting persons suspected of TF). The NCTV is in charge of the co-ordination of the Strategy. At the time of the onsite visit, the NCTV was in the process of updating the National Counterterrorism Strategy. The new Strategy will not envisage any substantial change in the approach to TF.

246. The NCTV is also responsible for the compilation of regularly updated Terrorist Threat Assessments (DTN). The findings from TF intelligence and investigations are incorporated into the DTN, which is publicly available on the government website. The DTNs also ensure that the measures included in CT policy and the national Strategy remain up to date. Based on DTN findings, the authorities can develop flexible measures, in the form of inter-ministerial programmes or project plans. The threat assessments were used as a basis to develop the Comprehensive Action Programme to Combat Jihadism, and to set-up an inter-ministerial task force on problematic behaviours and unwanted foreign financing.[42] The findings from TF investigations contributes also to the TF NRAs, which inform risk-based policies and mitigating measures.

247. At the operational level, there is strong co-ordination and co-operation between the authorities in charge of terrorism and TF investigations, as described above. Several cases demonstrate the strong integration of financial intelligence in CT cases, and its usefulness to identify terrorist suspects and adopt successful enforcement actions in a timely manner, including the investigation presented in Box 4.5.

Box 4.5. Use of financial intelligence in a CT investigation

Terrorist attack on Utrecht tram

In March 2019, a lone actor shot four people and severely injured three in a tram in Utrecht. On the day of the attack, the OM released the suspect's name to the media. On this basis, a FI established that the attacker had registered in an online platform to obtain information about opening a business account. In the application, the suspect provided an address and a mobile phone number that were unknown to the police. The FI reported the transaction to the FIU-NL, which immediately declared it suspicious and informed the investigation team, the CT Infobox and the AIVD.

Based on the data contained in the reported suspicious transaction, in particular the telephone number and IP data, the Police were able to trace the mobile phone and location of the suspect. The suspect was arrested on the same day, thus preventing possible subsequent attacks. The individual was sentenced in first instance to life imprisonment for murder with a terrorist intent.

Effectiveness, proportionality and dissuasiveness of sanctions

248. The Netherlands prosecutes TF through three distinct criminal offences: the TF offence under WvSr, Art. 421, the participation (financing) in a terrorist organisation under WvSr, Art. 140a and the violation of the Sanctions Act (Sw, Art. 2-3). In practice, the penalties applied by the Court in TF cases are generally low, which limits their dissuasiveness. The Assessment Team based this conclusion on the statistics and the analysis of TF case studies provided by the authorities.

42 DTN analysis will also be used to counter the threat from right-wing terrorism.

249. The prosecution policy is that, as a rule, unconditional imprisonment must be demanded for TF cases. The prosecution can also request to apply additional conditions (e.g., surveillance or travel or contacts bans) depending on the merits of the case. As noted in the TC Annex, the maximum penalty for TF is eight years' imprisonment, or a fine of the fifth category, and fifteen years' imprisonment for the financing of a terrorist organisation. The violation of the Sanction Act is considered a serious economic offence, punishable by a maximum of six years imprisonment, community service or a fifth category fine.

250. The Netherlands' conviction rate for TF offences is approximately 70%. Twenty-seven individuals have been prosecuted for TF offences in the period between 2016 and 2021, with 19 convictions and eight acquittals. The majority of cases prosecuted so far involve the provision of funds to FTFs, often by relatives and involving small amounts. While this is largely in line with the country's risk profile, the sentencing applied in these cases is very low, with only a few months of imprisonment (see Box 4.1). In almost half of the cases, only community service or suspended prison sentences were applied (Table 4.1).

Table 4.1. Imprisonment sentences for TF-related convictions (per person)

	Sentencing for TF or violation of the Sanctions Act	Combined sentences [e.g. TF or violation of the Sanctions Act in combination with tax fraud or other offences]
Community service or suspended imprisonment	8	1
Under 1 year	4	3
1 < 2 years	-	1
2 < 3 years	-	2

Note: The length of the sentence includes only the unsuspended prison terms.

251. The highest sentences for TF-related convictions are the result of cumulative sentencing, where the TF offence is combined with other offences such as the participation in a terrorist organisation, committing preparatory acts with a terrorist intent, tax fraud and forgery. In the case of cumulative sentences, the Court's ruling refers exclusively to the overall sanction. Therefore, it is not possible to determine the specific sanction accorded to the TF component of the charge. However, even in these cases, the combined sentences are lenient, with the highest conviction being 30 months of imprisonment, with an additional suspended sentence of twelve months. Therefore, the Assessment Team does not consider the sanctions applied in practice for TF to be dissuasive.

4

Box 4.6. Examples of TF cases with the highest sentencing

Support to a terrorist network in Syria

The case concerns three suspects in the Netherlands supporting terrorists in Syria by making money, telephones and laptops available. The investigation began in mid-2014 and was completed in February 2015. Evidence against the suspects included the analysis of transaction data from FIs, FIU-NL, FIOD and a money transfer service. In 2016, one of the suspects was convicted of TF, conspiracy to prepare terrorist offences and participation in a terrorist organisation, to 30 months of unconditional imprisonment, and 12 additional months on probation. The other two individuals received lower sentencing: 16 months, and eight additional months on probation for participation in a terrorist organisation, and six months imprisonment, with six additional months on probation, for TF.

Providing EUR 17 000 to a FTF in Syria

Between 2013 and 2014, an individual used intermediaries to send nearly EUR 17 000 to his brother, who was fighting with ISIL in Syria and who was placed on the National Terrorism List. The individual deliberately provided incorrect data to the Tax Administration and wrongfully received a sum of money in excess of EUR 10 000, the majority of which was transferred to his brother in Syria. In 2017, the Court sentenced him to a term of imprisonment of 24 months, of which 14 months are suspended on probation, and special conditions, for TF, violation of the Sanctions Act 1977, the Al-Qaida Sanctions Regulation 2011, the Terrorism Sanctions Regulation 2007-II, and forgery of documents.

252. In terms of TF sentencing, there are no specific TF guidelines for the OM, nor sentencing orientation points for judges. The Court will take into consideration several factors to determine the final sentence, including the severity of the case, the amount involved, the relationships amongst subjects, and past sentencing for similar offences. While this low level of sentencing is partly related to the personal motive (e.g., support provided to family members), rather than ideological, the relatively low frequency and amounts involved, and the heavier weight put on preventive measures and the integration and rehabilitation of the offenders (see also IO.7 in relation to the authorities' approach to criminal sanctions), the Assessment Team considers the level of sanctions applied for TF in practice not dissuasive.

Alternative measures used where TF conviction is not possible (e.g. disruption)

253. The authorities make use of a range of alternative criminal justice, regulatory and administrative measures when it is not possible to achieve a conviction for TF. The Table of Four examines available evidence to decide whether to pursue a TF charge. When there is insufficient evidence, the Table of Four can decide to send a case back to the Police and/or FIOD to request additional investigation. If there is no further investigative lead to explore, it can request the Police, FIOD, AMLC, or the OM to investigate/prosecute alternative charges, such as tax fraud or ML.

254. In the interest of national security, Dutch authorities can also revoke the Dutch citizenship of individuals who joined a terrorist organisation. This measure can apply to persons who joined Al-Qaida, Ahrar al Sham or ISIL, and in possession of a second nationality and 16 years of age or older. The revocation can be based on AIVD reports, a conviction for a terrorist offence, or other information such as foreign judgements. This measure has been applied to 17 individuals as of 18 November 2021.[43]

255. The Netherlands also adopted an Act on Termination of Benefits, Student Finance and Allowances in the Event of Participation in a Terrorist Organisation. This is an administrative measure to ensure that the State does not finance terrorism. The measure was introduced as the majority of FTFs were receiving some form of government support. Municipalities initiate the termination of the benefits on the basis of intelligence received from the CT Infobox, as described in the example below.

Box 4.7. Termination of public benefits and allowances for FTFs

Between 2013 and 2017, many individuals left for Syria and Iraq to join ISIL as FTFs. The CT Infobox actively monitored these subjects. In some cases, it turned out that emigrated subjects were not removed from the municipal registers. Therefore, the CT Infobox advised the Police to alert the local authorities/municipalities. As a result, the individuals were cancelled from the municipal register and social benefit allowances were stopped.

256. Since 2017, the Netherlands imposes a range of administrative measures, including a requirement to report, a prohibition of contact, an electronic monitoring or a travel ban to individuals linked to terrorist activities or supporting these activities, as per the Counter-Terrorism (Interim Administrative Measures) Act.[44] These measures are not dependent on a TF conviction. Measures such as travel ban or passport withdrawal can be imposed to individuals who intend to leave the country to join terrorist organisations. Between 2017 and 2021, these types of measures were imposed on 11 individuals.

257. The Netherlands has also undertaken initiatives to prevent the undetected return of FTFs. It has included known FTFs in the Schengen Information System and in the list of wanted persons and has cooperated closely with its European partners within Frontex and EUROPOL. It has also informed regional authorities, intelligence services, KMar with a view to identifying any returnee who attempted to travel back to the Netherlands. In relation to returnees, the Netherlands has an integrated approach to determine the best strategy (e.g., a criminal and/or intelligence investigation or reintegration initiatives).

---

[43] This measure has a sunset clause of 1 March 2022. However, the authorities informed the team that the Senate is considering a bill to extend it for an additional five years. The deprivation of citizenship was also applied to 20 individuals, as an additional measure upon conviction for a terrorist offence.

[44] Based on the current threat picture, the Dutch government will extend the Act for a period of five years, until March 2027. At the time of the onsite, the Bill was before the Senate.

4

Overall conclusions on IO.9

The Netherlands has a strong understanding of its TF risks and a robust institutional framework to ensure the detection, investigation and prosecution of TF. The number and features of the TF cases investigated and prosecuted are largely consistent with the country's risk profile, even if further efforts are needed to successfully prosecute NPOs linked to TF. The authorities demonstrated the ability to use alternative criminal or administrative measures where a TF conviction cannot be secured. However, the Assessment Team does not consider the sanctions applied in practice for TF to be dissuasive.

The Netherlands is rated as having a substantial level of effectiveness for IO.9.

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

258. Overall, the Netherlands implements TF TFS without delay and makes use of domestic designations, largely in line with its risk profile; however, some shortcomings remain, particularly in relation to the implementation of TFS by certain categories of DNFBPs and the communication of changes to the lists, which does not always occur without delay. As described under R.6, the Netherlands implements TF TFS through EU decisions and regulations, complemented by domestic legislation. To overcome the delays in the transposition of UNSCR designations at the EU level, domestic 'bridging legislation' ensures that UN designations are in force in the Netherlands (including BES Islands) from the date of their publication by the UN, until the EU provisions enter into force.

259. In addition to UN TFS, the Netherlands implements EU and domestic designations related to TF. At the EU-level, at the time of the onsite visit, the terrorism sanctions list (under CP 2001/931 - CR 2580/2001) included 15 individuals and 21 entities, and the autonomous EU-regime for ISIL and Al-Qaida (under CD 2016/1693 - CR 2016/1686) included six individuals. At the domestic level, the Netherlands has designated 145 individuals and two entities. The obligation to freeze funds takes effect immediately upon the publication of the designations in the national Gazette.

Designations

260. The Netherlands has an effective multi-agency framework in place to identify targets for designations. The Minister of Foreign Affairs is the responsible authority to designate an individual domestically, and to submit proposals to the UN Sanction Committees, the EU COMET or to third countries. It acts in co-ordination with the Ministers of Finance and Justice and Security, and after consultation of the Asset Freezing Committee (BVO). The Asset Freezing Committee convenes on a regular basis (every one or two months) to discuss designation proposals. The participation of the OM[45], AIVD, FIU-NL, and NCTV enables the Committee to consider all relevant financial and non-financial intelligence in its determinations.

[45] For the BES Islands, the OM Carib will also participate.

261. Generally, the OM and AIVD submit nomination proposals and initial supporting information to the Committee, while FIU-NL intervenes to provide additional information on a specific target. As a standard practice, in all cases FIU-NL consults iCOV, to gather a comprehensive assessment of the target's financial assets, or possible relevant connections. NCTV also regularly consults local actors, such as municipalities and presents relevant information to the Committee. In practice, authorities, in particular the OM, have discretionary powers to decide whether to propose a name for listing. This power is not always associated to the application of clear listing criteria to decide whether to propose a name for domestic, EU, UN or third country designation and may lead to missed opportunities to prevent terrorists, or their supporting network, from raising funds. The Netherlands may also opt for other types of criminal or administrative measures, as described under IO.9.

262. The Dutch national sanctions list includes mostly FTFs who left the Netherlands to fight in Syria and Iraq and join terrorist groups, such as ISIL and Al Qaida. The two entities listed at the time of the onsite visit were charitable foundations suspected of indirectly providing financial support to terrorist organisations. The composition of the sanction list is largely in line with the country's risk profile, although the Assessment Team expected more NPOs on the national list, given their high-risk categorisation in the TF NRA. At the time of the onsite, the Netherlands had proposed two designations to the EU CP931 list, and one designation to the EU ISIL and Al-Qaida list. The Netherlands had co-sponsored the designation of one individual and three entities under the 1267/1989 regime, but it had not made any designation proposals of Dutch nationals to the UN sanctions Committees, nor to third countries.

263. The Netherlands considers third-party requests through the same procedure applied to domestic designations proposals. Out of the fourteen requests received between 2015 and 2020, it has listed only one person (see Box 4.8), as it will proceed with a listing only if it is possible to establish a link between the proposed subject and the Dutch system (e.g., indications that the subject is engaged in terrorist acts in or from the Netherlands, or in facilitating such acts, or in making or facilitating transactions via the Dutch territory, or Dutch nationals or legal entities).

Box 4.8. Domestic designation pursuant to a third country request and designation proposal to the EU

In October 2016, the Netherlands listed an individual because of their association with a terrorist organisation active in the Middle East, and upon a request from a third country. The AIVD conducted independent research into the subject, which led to the identification of reasonable grounds for designation. After consultation of the BVO, the Ministry of Foreign Affairs listed the individual. Based on the AIVD information, the individual was found to be involved in a European network. The Netherlands subsequently submitted a listing request to the EU terrorism sanction list. The proposal was discussed in COMET and agreed at the beginning of 2017.

Communication of designations

264. There are tools available to communicate new designations to obliged entities. For UN and EU designations, the Netherlands relies on the publication of the EU designations in the EU Official Journal. A consolidated list is also available on the EC website and obliged entities can subscribe to the EU financial sanctions database. However, not all Dutch obliged entities do so, and there is also a delay of a few days between the UN designations and the publications by the EU. While most FIs and some DNFBPs rely on commercial databases to screen for TFS, the lack of more proactive communication channels could hamper the timely implementation of TFS by some obliged entities. National designations are published in the Government Gazette and the Government publishes a consolidated national sanction list on its website and on the website of the Ministry of Foreign Affairs. The Ministry of Foreign Affairs has a notification system in place, alerting any modifications to the national list to subscribed FIs and DNFBPs. However, not all obliged entities are registered and the list does not cover EU/UN designations. DNB and AFM publish updates on the national and EU designations in a monthly newsletter to subscribed FIs and DNFBPs. There are approximately 5 000 subscribers. When new persons or entities are added to the national list, in the period in between the monthly newsletter, an additional newsletter about these designations is sent out, but this notification may also occur with a delay. All DNB newsletters are also available on DNB's website. Since this communication comes with a delay, entities relying on it (particularly smaller FIs and DNFBPs) may implement TFS with a delay.

Implementation of sanctions

265. Between 2015 and 2020, the Netherlands froze around EUR 17 150 under the UN 1267 list, EUR 177 under the UN 1988 list, and EUR 58 710 under the national list. These relatively low amounts are consistent with the terrorism and TF risk profile of the country (mainly microfinancing of FTFs). As noted above, the obligation for any person and all obliged entities to freeze funds starts immediately from the moment of the publication of a designation by the UN, by the EU on the EU Official Journal or in the national Gazette for domestic designations.

266. FIs and some DNFBPs have a good understanding of the general obligations related to TFS. This was confirmed by the interviews held during the onsite visit. As noted under IO3, since DNFBPs other than trust offices are not supervised for TFS implementation, it is difficult for the authorities to assess whether, in practice, all DNFBPs understand and implement their TFS obligations without delay. The same applies to certain categories of DNFBPs and VASPs in the BES Islands.

267. The Netherlands does not maintain statistics to assess whether obliged entities froze and reported any funds or assets belonging to a designated individual or entity without delay (see also IO4). However, the authorities provided two examples to the Assessment Team, where FIs reacted immediately to new designations on the national list, and froze the funds on the same day. The FIs also promptly communicated their actions to DNB and the Ministry of Finance.

268. While all obliged entities are required to freeze the assets of designated individuals or entities, the Assessment Team considers the lack of an explicit obligation for certain categories of DNFBPs to report frozen funds, and to have a sanction screening system in place to screen their clients against the sanction lists as deficiencies.

269. The Netherlands has developed effective mechanisms to regularly reconsider the listing or de-listing of domestic designations, as well as to authorise exemptions pursuant to UNSCR 1452. Since 2016, the authorities de-listed 20 individuals and two entities. The Netherlands granted 33 exemptions, mainly to cover basic living expenses and to pay certain taxes or utility bills.

270. To facilitate TFS implementation, the authorities provide guidance through information available on their websites, as well as guidance papers, newsletters, circulars and other policy statements. In addition, there are two public-private platforms to discuss TFS-related issues. Firstly, the Sanctions Expert Pool brings together representatives of larger banks, DNB and the Ministry of Finance to discuss TFS implementation. Secondly, in the Financial Sanctions Network, the Ministry of Finance discusses issues related to TFS with representatives from non-bank FIs and TCSPs.

271. Over the past few years, DNB and AFM conducted thematic investigations into TFS compliance in multiple sectors. The FIOD has actively investigated violations of the Dutch sanctions law and in several TF cases, individuals were convicted for providing funds to listed FTFs (see IO.9).

Targeted approach, outreach and oversight of at-risk non-profit organisations

Understanding of the risk and mitigating measures

272. Both the 2017 and 2020 TF NRAs identify the financing via foundations or other legal entities, including national and international fundraising, as the greatest TF risk in the Netherlands. The authorities have undertaken significant work to determine the subset of NPOs most vulnerable to potential TF abuse.

273. In the Netherlands, there are approximately 266 109 foundations and 131 676 associations.[46] Within these groups, the Netherlands considers those NPOs acting with a charitable purpose as the subset falling within the FATF's functional definition of NPO. The authorities assess that most of these NPOs are posing a low risk, notably the ones with ANBI status and CBF recognition. Using terrorism and TF intelligence, the authorities identified a small subsector of organisations at higher risks of potential TF abuse. The features of NPOs at higher TF risks include:

- foundations with potential ties to jihadist groups;
- NPOs operating in or close to areas where terrorists operate;
- NPOs financed by foreign radical groups to influence certain religious foundations in the Netherlands;
- NPOs abused to collect funding (e.g., for aid projects) in the Netherlands to finance TF both in the Netherlands and abroad.

[46]. As of 15 November 2021.

4

274. The authorities' understanding of TF risks for the NPO sector was informed by the NRA results, the NCTV DTN (see IO.9), TF signals and investigations involving NPOs, FIU-NL research, which also led to guidance and indicators for obliged entities, as well as information provided through public-private partnerships (see Box 4.9). Between 2015 and 2020, FIU-NL investigated UTRs involving approximately 1 100 foundations and found that 50 could be linked to terrorism or TF. During the discussion with the authorities, it emerged that associations are considered to pose a considerably lower TF risk than foundations, as they have not yet been implicated in TF signals detected by the authorities.

Box 4.9. Initiatives to detect the abuse of NPOs for TF purposes

Public-public

FEC TF Programme (see Box 4.2): the programme enables participating government agencies to share information and insights into networks and methods of financing of suspected individuals, including NPOs. The analysis of TF subjects shows that returnees are sometimes involved in foundations and small businesses.

Public-private

FEC TF Task Force (see Box 4.2): this partnership allows LEAs to share concrete signals and operational information on specific subjects (including NPOs) for which there is not yet a clear suspicion, with five banks and one insurance company, for them to search whether they have any UTR or relevant information in their system.

FEC Rogue Foundations project: it started in 2018 to share knowledge on the misuse of foundations, including for TF. It involved four major banks, AMLC, FIOD, FIU-NL, Police and OM. It led to the identification of a risk profile and red flag indicators to detect UTRs, and in the development of a barrier model to prevent the abuse of foundations.

TF Platform: every 6-8 weeks, FIU-NL and four participating banks share anonymised information on previous TF cases – including those involving NPOs, to support FIs in assessing risks of money flows. This information enabled the FIU-NL to identify 50 NPOs possibly linked to terrorism and TF.

275. Notwithstanding these important initiatives, there is room for further improvement in the authorities' ability to identify NPOs at high risk for potential TF abuse. For instance, the Netherlands has not conducted a separate sectoral assessment of its NPO sector. The authorities met during the onsite had difficulties in obtaining a clear and comprehensive insight into the number of NPOs that might pose a high TF risk. In particular, there is no clear information on how many of the 266 109 foundations are set up for charitable purposes (versus other non-charitable purposes). Consequently, it is impossible to determine the number of charitable foundations operating without an ANBI status or CBF seal. This is key information, as the charitable foundations without any of these statuses are not subject to any standard or transparency requirements, and could therefore be highly vulnerable to abuse.

276. Furthermore, the Assessment Team has some concerns in relation to the limited requirements applicable to church communities. Due to the principle of separation between church and state, the authorities are reluctant to require transparency or perform strict controls on these organisations. Church communities have no obligation to conclude a notarial deed for their establishment, and they are not subject to the Wna (see IO.5). Some obliged entities met during the onsite mentioned church communities as high risk for illegal activities and referred to cases where this legal form was used for non-religious activities.

Outreach to the sector and its understanding of the risk

277. The Netherlands has demonstrated a proactive approach in engaging NPOs in outreach activities, which increased the sector's awareness of its potential vulnerabilities to TF abuse. The authorities have worked very closely with NPOs, in the development of best practices to address TF risks and vulnerabilities. In June 2021, the Ministry of Finance, in co-operation with NPOs branch organisations and CBF, published a factsheet to support NPOs in recognising and preventing TF abuse. The FIU has also developed a non-public factsheet specifically addressed to gatekeepers, with 66 confidential indicators to help them monitor NPOs transactions with a risk-based approach.

278. The Ministry of Finance, the Ministry of Justice and Security, the Ministry of Foreign Affairs and the Human Security Collective (HSC) have also held a series of roundtables to establish a public-private dialogue, exchange information and discuss issues related to TF risks and NPO de-risking. An overview of the roundtables is presented in Box 4.10. These initiatives were open to all NPOs and involved those NPOs operating in good faith, which are most vulnerable to potential TF abuse due to their activities (e.g., organisations operating in or close to conflict zones, with an active terrorist presence). Between January 2016 and November 2021, ten roundtables were organised.[47]

[47] The Netherlands aims to organise two roundtables per year. Due to the COVID19 pandemic, in 2020 and 2021 it was possible to organise only one roundtable per year.

4

Box 4.10. NPOs roundtables

Since 2016, the Ministry of Finance, the Ministry of Justice and Security, the Ministry of Foreign Affairs, the HSC, have regularly organised round tables on the themes of de-risking and financial access for NPOs, CFT policy and FATF standards. The round tables are open to NPOs of different sizes and to the Dutch Banking Association. This public-private dialogue gives government agencies, supervisors, banks and NPOs opportunities to gain a clearer understanding of TF risks, the effect of CFT regulations on civil society organisations, and prompt the development of shared solutions.

On average, a subset of 10 to 20 NPOs (most of which are umbrella organisations representing several members) participate in each round table. HSC communicates the outcomes of the roundtables within their network via bimonthly newsletters, which are sent to approximately 200 NPOs and shares updates online. The roundtable organisers also seek to establish relations with roundtables organised in other countries, and international roundtables promoted by international organisations such as the World Bank or EU.

279. NPOs met by the Assessment Team—including organisations which, by virtue of their activities, are more exposed to TF threats—were well aware of TF risks. They have effective mitigation measures in place, such as procurement procedures, vetting of staff and partners on the ground, and performing checks on donors, beneficiaries and partners against the sanctions lists. NPOs, in particular umbrella organisations, are actively involved in promoting awareness and good practices to counter TF abuse within the non-profit sector. NPOs confirmed that there is a good dialogue with the Dutch authorities and the banking sector. While appreciative of the current engagement with public and private sector entities on de-risking, they also stressed that, in some cases, they were experiencing persistent challenges to access vital financial services to perform their charitable activities abroad (particularly in or near conflict zones).

Oversight and action taken

280. The Netherlands gives a prominent role to self-regulation. As such, there is no government authority in charge of supervising the non-profit sector. There are initiatives and tools that contribute to reducing the risk of TF abuse within the sector, but they are not part of a general policy or coordinated action plan.

281. There are several moments in the life-cycle of a NPO where some forms of screening are carried out (see c.8.2). All associations and foundations (including NPOs) must be established via a notarial deed and register with the CoC's Company Register. As noted above, this obligation does not apply to church communities. This registration and the obligation to register changes to the information in the CoC's Company Register will trigger screening via JustisTRACK whereby NPOs with a high TF risk may be identified, for example, when persons on a terrorist sanction list or with criminal records are involved in the NPO (see IO5). NPOs are also subject to CDD measures by obliged entities when opening a bank account.

282. In the Netherlands, there are two voluntary certification systems rewarding NPOs (including in the BES Islands) that fulfil certain requirements in terms of transparency and accountability:

i. **ANBI (Public Benefit) status**, which also provides certain tax exemptions to stimulate charity. The Tax and Customs Administration delivers the status to NPOs fulfilling accountability, integrity and transparency standards. 53 565 organisations in the Netherlands[48] and 12 out of 717 associations and foundations in the BES Islands have the ANBI status.

ii. **CBF (Fundraising Accreditation) seal** is a quality label for NPOs that want to raise funds. The Fundraising Accreditation Agency (CBF) delivers this status to NPOs fulfilling a set of requirements in terms of accountability, integrity and transparency. 655 organisations have CBF certification. In terms of volume, these organisations represent a large share (80%) of the total funds raised. The controls in place for the CBF are stronger than for the ANBI status.

283. However, for NPOs other than those with an ANBI status or CBF recognition, there is no obligation to make financial statements available to the CoC, record their transactions, or undertake similar measures to ensure transparency in their operations, nor is a supervisory mechanism in place.

284. Organisations which voluntarily agree to be part of umbrella NPOs have self-regulation requirements, or codes of conduct. Both the outreach by the government and the voluntary certification systems mainly reach the 'good faith' NPOs with legitimate charitable activities. Some obliged entities indicated that they will only accept charitable foundations with ANBI status or CBF seal as clients, as other charitable foundations are considered too high risk.[49] Non-compliance with ANBI or CBF transparency criteria (or membership criteria of an umbrella organisation) may lead to these labels being revoked, but, aside from losing advantages, there are no real sanctioning measures in place, such as fines.

285. While self-regulation and voluntary certifications are suitable to increase transparency and accountability within good faith NPOs, 'bad faith' organisations (i.e., NPOs that deliberately give up tax advantages to avoid any transparency and accountability requirements linked to the voluntary certification system) can easily escape from any control on the use of their funds. LEAs are often unable to investigate foundations, as it is difficult to gather evidence due the lack of transparency and accountability requirements. With the exception of the two NPOs placed on the domestic sanction list, criminal prosecution seems to be the only way to act against foundations suspected of TF. Moreover, it is very difficult to dissolve NPOs complicit in TF, with the result that, in practice, they can continue with their activities and raise funds unless a criminal conviction is achieved. As noted under IO.9, at the time of the onsite visit, no NPO had been convicted for TF.[50]

---

48 32 762 foundations and 2 723 associations. Organisations with an ANBI status include also other types of legal entities, such as public legal entities and church communities.

49 The Netherlands is considering to develop a digital portal for NPOs to increase access to financial services. There are ongoing discussions between CBF and the banking sector to establish a website where all charities can do a self-assessment of their risk profile, with a view to facilitate their access to bank services.

50 At the time of the onsite visit, a draft law to increase transparency of civil society organisations (WTMO law) was under review by the House of Representatives and the

286. In the BES Islands, the NRAs concluded that the level of TF risk is low and no specific TF risks are associated with NPOs. There are no specific measures or actions taken to NPOs, which suggests that the authorities consider that they pose no risk.

Deprivation of TF assets and instrumentalities

287. The Netherlands mainly relies on the use of national designations and freezing measures to counter FTFs, with the high majority of funds frozen under the national list (EUR 58 710) and less important sums pursuant to UN designations (EUR 17 150 under the 1267 list; EUR 177 under the 1988 list). As noted under IO.9, the authorities have also made use of administrative measures, such as the halting of social benefits, to deprive terrorists and their support networks of any assets.

288. The seizure and confiscation of terrorist assets and instrumentalities during TF investigations has yielded minimum results, with an estimate of only a few thousand EUR seized under suspicion of ML rather than TF. The authorities mentioned a number of challenges in pursuing confiscation of terrorist assets, including that in most terrorism or TF investigations, the money is already in the conflict zones and is therefore impossible to seize. Furthermore, when the money is collected under the cover of a charity, the authorities struggle to collect sufficient evidence to initiate a TF investigation, due to the lack of any legal requirement for transparency and accountability of foundations.

Consistency of measures with overall TF risk profile

289. The measures undertaken by the Netherlands are largely consistent with its TF risk profile. These conclusions are based on the analysis of the NCTV terrorism threat assessment, and the findings of the TF NRAs. The Netherlands has used domestic designations and asset freezing measures to target FTFs and their supporting network, which is consistent with the findings of the NRAs.

290. The Netherlands has also taken action to address the abuse of NPOs for TF purposes, which is the main TF risk identified by the authorities. It has conducted extensive outreach initiatives and has established a robust dialogue and co-operation with good faith NPOs most vulnerable to TF abuse. It has invested in intelligence and public-private partnership to detect the possible abuse of NPOs. However, the limited controls in place for some NPOs and the lack of a comprehensive assessment of the sector hamper the ability of LEAs to detect and prosecute organisations wilfully supporting terrorism.

Council of State. The law would require foundations to file their internal financial records within the CoC. It would also allow mayors or the OM to request civil society organisations to disclose information on their financial flows (donations), in some specific circumstances, and temporarily freeze, prohibit or confiscate some funds/financial flows. It would also allow to impose penalties in case of lack of co-operation.

Overall conclusions on IO.10

The Dutch legal framework ensures that UN designations are immediately applicable in the Netherlands and BES Islands. All natural and legal persons, including all FIs and DNFBPs, are under an obligation to implement TFS. However, the lack of certain specific obligations relating to TFS for certain DNFBPs sectors, creates a potential gap in the implementation of TFS without delay. The communication mechanisms in place may not always ensure a prompt communication of new designations, in particular UN and EU ones. The Netherlands has primarily used its domestic sanction lists to designate FTFs, which is in line with the risks. The low amount of TF assets frozen is also consistent with the TF activities in the country.

The Netherlands has proactively engaged with good faith NPOs to raise awareness on TF risks and vulnerabilities. It has provided good practices to both NPOs and the private sector to help detecting transactions potentially related to TF, and limiting de-risking. Good faith NPOs at risk of TF abuse are aware of their risk and have mitigating measures in place. The authorities have a robust understanding of the subset of organisations posing higher TF risks. However, a more granular assessment is hampered by the lack of a sectoral risk analysis and the limited visibility on the financial activities of those NPOs which are not part of any voluntary certification scheme, and therefore not subject to supervision. Overall, the Immediate Outcome is achieved to a large extent.

The Netherlands is rated as having a substantial level of effectiveness for IO.10.

Immediate Outcome 11 (PF financial sanctions)

291. While not presently required under the FATF Standards, in 2020, the Netherlands conducted an initial assessment of its PF risks, threats and vulnerabilities through the "Proliferation Financing Monitor". This exercise contributed to the authorities' understanding of the risks and exposure to PF activities. The authorities are aware that some characteristics of the Dutch economy—in particular, the country's position as a trade hub and its large financial sector—could potentially expose it to PF. However, the Netherlands is geographically distant from both Iran and DPRK and there are no intensive trade relationships with these two countries. The import-export activities are almost negligible with DPRK. The import-export with Iran corresponds to a minimal part of the overall Netherlands' trade flows, but still accounts for an annual average of EUR 187 million of imports, and EUR 626 million of exports, mainly in relation to mineral fuels (import) and raw materials, machinery and transport equipment (export). There are very limited financial transactions made from and to Iran and DPRK. The share of proliferation-sensitive incoming and outgoing transactions by banks is very low, when compared to the total number of transactions conducted (>0.0001%).

292. The Netherlands considers that the direct implementation of PF sanctions at the European and Dutch levels, combined with limited financing and trade flows, results in an insignificant risk of PF sanctions being violated. Due to the limited number of cases related to PF, the authorities have not yet identified any specific typology for PF sanction evasion. However, they consider that the use of shell companies and VAs continues to pose a risk.

293. The Netherlands has an export control system in place for the exportation of controlled goods and technologies related to dual-use goods.

294. The North Korea Sanctions Regulation 2017 designates the Ministry of Finance, the Ministry of Education or the Ministry of Foreign Affairs as the authorities responsible for CPF issues related to DPRK. The Iran Sanction Regulation 2012 identifies the Ministry of Finance, Ministry of Economic Affairs and the Ministry of Foreign Affairs as the competent authorities for the implementation of CPF measures related to Iran. As noted under IO.1 (see Table 1.1), the Netherlands has solid inter-agency co-ordination in place to discuss sanctions' implementation, including on PF, and to share relevant information and best practices with the private sector (and banks, in particular). Amongst the different mechanisms, the Carré Consultation has a specific focus on PF, and enables all authorities involved in import and export controls to exchange information and discuss real cases.

Implementation of targeted financial sanctions related to proliferation financing without delay

295. As an EU member state, the Netherlands relies on the EU framework for the implementation of TFS related to Iran and DPRK. Similar to TF-related TFS, national bridging provisions enables the Netherlands to implement PF TFS without delay. Any new UN designation is immediately in force in the Netherlands (including the BES Islands) from the moment of its publication by the UN, and until the corresponding designation by the EU enters into force. In addition to the UN designations, the Netherlands also applies the additional sanctions on DPRK and Iran imposed by the EU to bolster UN sanctions and prevent their circumvention. The Netherlands adopts the same mechanism described in IO.10 for the implementation of PF-related sanctions.

296. The same considerations noted in relation to the prompt and proactive communication of TF designations apply to PF TFS (see IO.10 for detailed analysis) and may affect the ability of certain obliged entities to implement TFS without delay. In particular, not all obliged entities use automatically updated commercial databases for sanctions screening, subscribe to the UN or EU notification systems or the DNB and AFM newsletters to receive timely updates on new designations, and the implementation of TFS without delay by DNFBPs, with the exception of trust offices is not supervised.

Identification of assets and funds held by designated persons/entities and prohibitions

297. At the time of the onsite visit, the Netherlands had not made any listing or delisting proposals to the relevant UN Committees. Very few assets were frozen pursuant to UN designations related to Iran (EUR 483). In relation to DPRK, the Netherlands recorded a major freezing of over USD 16.3 million, carried out by an Asian branch of a Dutch bank and two smaller frozen amounts of USD 26 and EUR 78. The limited amounts of frozen assets in the Netherlands is consistent with the low exposure to PF. Nevertheless, the lack of certain specific obligations relating to TFS for certain categories of DNFBPs in the Netherlands, with the exception of trust offices, and DNFBPs in the BES Islands and the lack of obligation to report any positive sanction hits to their supervisor, creates a potential gap in the implementation of PF-related TFS.

298. In case of a positive hit, FIs, VASPs and trust offices are required to immediately freeze the assets and report the match to DNB or AFM. The supervisors assess the reports on their completeness and forward them to the Ministry of Finance for a second assessment. The assets must remain frozen, until further notice is provided to the FI or trust office.

299. Between 2016 and 2021, DNB received 15 reports on possible "hits" with sanctioned individuals and entities in Iran and DPRK. In seven cases, assets were frozen. In the other eight cases, it was impossible or inapplicable to freeze the assets, for example because the reporting institution was an insurer and no credits were paid out yet. The majority of the reports—nine out of 15—were related to Iran. With the exception of the USD 16.3 million freezing in Asia, the identified matches involved very small amounts of funds, between 1 and 78 EUR.

300. With a view to detect PF-related activities, the Netherlands monitors trade movements possibly related to PF and the corresponding money flows. In several occasions, customs have intercepted and prevented suspicious goods, possibly related to PF sanctions, to reach their final destination, as illustrated in the case example below (Box 4.11).

Box 4.11. Shipment of luxury items directed to DPRK

On the basis of intelligence and information provided by an international partner, the transport of a shipment of containers was halted in the Port of Rotterdam. Based on intelligence, the ultimate destination of the shipment was the DPRK. Even though there were suspicions of the sanctions against DPRK having been violated in this case, there was a lack of evidence. The authorities reached an agreement with the shipping company to return the containers to the seller, but in the end the goods were destroyed.

301. The Netherlands has procedures in place to deal with exemptions authorised by the relevant UN resolutions. In practice, the Netherlands has granted few exemptions under the EU Iran regulation, related to the payment of legal fees.

FIs, DNFBPs and VASPs' understanding of and compliance with obligations

302. FIs, VASPs, trust offices and some other DNFBPs understand their general obligations to implement TFS, including on PF. However, while the Sanctions Act establishes a general obligation for everyone (i.e., all persons and obliged entities) to freeze assets and make no funds available, there is no explicit obligation in the Supervision Sanction Act for DNFBPs other than trust offices to screen for sanctioned individuals or entities. Many DNFBPs interviewed during the onsite indicated that they do screen their clients against sanctions lists. Even in cases where a DNFBP did identify a sanctioned person or entity as a part of its CDD processes, it is unclear whether this information would reach the Ministry of Finance. The lack of certain specific obligations relating to TFS for certain DNFBP sectors and to report any match and the subsequent lack of supervision hamper the Netherlands' ability to have a comprehensive view on all assets frozen or other actions taken to implement TFS.

303. The considerations on the level of understanding and compliance with TFS obligations are equally applicable to TF and PF TFS. The level of understanding and compliance between FIs is generally high, with most carrying out their screening and reporting any match to the relevant supervisor. FIs and trust offices have administrative and internal control measures to comply with sanctions regulation, screen any possible match with designated persons or entities, and report immediately a match to DNB or AFM. Many FIs also assess sanction evasion risks as a part of their Systematic Integrity Risk Analysis (SIRA), and of their obligation to determine an integrity risk score for each client, but this is less the case for trust offices.

304. In relation to insurer branches, a DNB off-site review in 2016/2017 revealed that approximately 75% of the population was compliant with the Sanctions Act and screened their clients against the national and EU sanction lists. The non-compliant institutions were required to remediate and set-up screening processes. They subsequently reported to DNB to confirm that they had remedied the identified deficiency. This resulted in 89% of them having specific policy on sanctions' screening by 2019. Furthermore, the insurers' trade association (VNAB) supports insurers' effective compliance with the sanctions regulations through a sector-specific online platform (see description in the Box 4.12 below).

Box 4.12. The insurers sanctions platform

The VNAB Sanctionpl@tform was launched in 2016. The platform identifies (prospective) business relations and checks them against all sanction lists. The standardised and computerised operation of the online application facilitates sanctions' compliant reviews, which are stored on the platform and accessible to co-insurance market parties. The platform fully supports CDD and Transaction Due Diligence reviews required by EU regulations. The platform is web-based and designed to be used for co-insurance, authorised underwriting and non-bourse policies, and accessible by both members and non-members of the VNAB. The platform supports the automated search of organisations and their BOs and checking them against the sanction lists in the context of CDD. In the context of Transaction Due Diligence, the platform supports the verification of whether the policy directly or indirectly relates to countries, products, or services included in the sanctions lists. The system is regularly tested for known positives and false positives.

305. As part of their new registration requirement, VASPs are generally aware of and understand TFS obligations. Sanctions evasion risks are part of their SIRAs. Due to the very recent supervision of the sector, a comprehensive picture on their level of compliance is not yet available.

306. The interviews with DNFBPs other than trust offices during the onsite visit revealed that most screen their clients against sanctions lists, even in the absence of an explicit obligation to do so, and report information to FIU-NL and/or Police. Between 2015 and 2021, the FIU-NL received three reports from DNFBPs referring to proliferation-related activities. These transactions were reported for ML reasons, but contained also a possible PF component related to dual-use goods. The Assessment Team notes that the supervision and guidance provided by DNB and AFM to the obliged entities under their supervision resulted in improved compliance and implementation with TFS obligations. In the absence of supervision for the majority of DNFBPs, there is therefore a risk that some shortcomings in the compliance with TFS obligations may persist for those categories of DNFBPs. It is also unclear whether DNFBPs other than trust offices understand the specificities of different sanction regimes (e.g., in relation to PF), or to which extent they are aware of the most common typologies of sanctions evasion.

307. As noted under IO.5, there are some challenges for obliged entities in identifying the BO, especially when international complex structures are involved. The Assessment Team notes that this may also result in a risk of sanctions evasion if the sanctioned person is the BO of a customer, or transaction. This risk is mitigated to a limited extent by the implementation of the additional sanctions imposed by the EU in relation to both DPRK and Iran.

308. In the BES Islands, supervised obliged entities generally understand and comply with the TFS obligations. However, as noted in IO.3, the lack of supervision for the implementation of TFS obligations by VASPs and DNFBPs other than trust offices also impact on the ability to understand the level of implementation and understanding of TFS obligations by these entities.

4

Competent authorities ensuring and monitoring compliance

309. The Ministry of Foreign Affairs provides general information on sanctions, and on the implementation of the Sanctions Act on its website. Factsheets and manuals are also available online to raise awareness on TFS obligations and on related topics, such as export controls. Guidance provided by government institutions as well as supervisors is mostly related to the implementation of TFS in general.

310. DNB and AFM, as supervisors for FIs, VASPs and trust offices, provided extensive and, where needed, sector-specific guidance to FIs, VASPs and trust offices on the implementation of TFS obligations, including PF. This includes DNB newsletters, notifications, seminars and information material published on the website. Furthermore, DNB issued a general guidance on the implementation of TFS, and a specific guidance on doing business with Iran. AFM is regularly in contact with obliged entities to answer any question via email, and issues monthly notices jointly with DNB, as well as guidelines.

311. DNB and AFM regularly check the organisation and effectiveness of the sanctions screening systems as part of their supervisory examinations. They have also conducted thematic investigations on the compliance with sanction regulations. While these are not specific to PF, they cover both the TF and PF component of the sanction measures. Whenever a breach is detected, DNB or AFM will provide additional guidance to the obliged entity and will follow-up on the remedial measures adopted. This has generally resulted in increased compliance with TFS obligations by both FIs and trust offices. For VASPs, due to the very recent supervision of the sector, a comprehensive picture on the level of compliance is not yet available. There is no supervision on PF-related sanction obligations by the supervisors of DNFBPs, with the exception of trust offices.

312. In terms of sanctions, there is effective co-ordination and collaboration between financial supervisors, FIOD and the OM, to ensure that any breach in the implementation of TFS is punished appropriately, either as an economic offence, or under criminal law.

313. DNB and AFM have not detected nor imposed sanctions for specific breaches of UNSCRs relating to PF. However, they did impose formal and informal measures for violation of the general obligations of the Sanctions Act to ensure that FIs and trust offices adopt remedial actions in the field of administrative organisation and internal control. In case of substantive violations, DNB and AFM exchange information with FIOD and the OM so as to determine the best approach on a case-by-case basis, as per the *una via* principle it is not possible to impose both administrative and criminal sanctions for the same violation.

314. In relation to DNFBPs other than trust offices, and DNFBPs and VASPs in the BES Islands, there is no supervision on the implementation of TFS obligations, including on PF. As a consequence, no control is performed on whether these categories of obliged entities understand or properly implement the sanctions, and the possible detection of PF TFS breaches is therefore left to LEAs.

315. The FIOD has investigated several violations of the sanctions provisions, and some legal persons were convicted for breaching PF-related sanctions. However, all cases investigated so far involve violations in the exporting of military or dual use goods, or exporting without a license, rather than the provision of funds/assets to listed individuals or entities.

Overall conclusion on IO.11

The Netherlands has a legal framework in place to ensure that UN designations are applicable in the Netherlands and in the BES Islands without delay. The lack of supervision of the implementation of TFS without delay for certain DNFBPs hinders the authorities' ability to assess the overall compliance of the sector with PF-TFS obligations. The communication mechanisms in place do not always ensure the prompt transmission of changes to the lists to all obliged entities. The results in terms of PF-related assets frozen are consistent with the country's low exposure to PF.

The level of understanding and compliance with PF TFS obligations is strong in the financial sector. The guidance and supervision provided by DNB and AFM resulted in increased awareness and compliance by the obliged entities under their supervision. It is unclear if all DNFBPs other than trust offices promptly implement PF-TFS, as implementation of PF-TFS is not supervised and there has been no specific guidance provided to these entities.

The Netherlands is rated as having a moderate level of effectiveness for IO.11.

Chapter 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

FIs and VASPs

1. Banks, larger MVTS and VASPs have a good understanding of their ML risks and obligations and regularly review their risk assessments. Understanding of risk in the insurance sector lags behind that of other sectors supervised by DNB and ML risk assessments are generally less developed for smaller and non-bank FIs. Understanding of TF risk is generally lower across all sectors.
2. FIs and VASPs generally apply mitigating measures commensurate with their risks. Many FIs have integrated mitigating measures, such as monitoring systems, but for some banks and MVTS there has been a tendency to categorise customers as low risk by default, which makes mitigating measures less effective.
3. Most FIs have appropriate policies and procedures in place commensurate with their risks. There has been significant investment in AML/CFT compliance in recent years and banks have improved controls, including ensuring strong ownership of AML/CFT issues at the senior management and board level.
4. CDD measures are generally well implemented, but some FIs including larger banks struggle to identify the ultimate BO, particularly when complex international structures are involved. This has been a focus of high profile enforcement action in recent years and the authorities are seeing improvements as a result.
5. FIs generally apply EDD in cases of higher risk and have automated systems to identify high risk customers and activities. However, in some lower risk sectors, such as life insurance companies and insurance intermediaries, a significant proportion of entities lack processes to identify PEPs.
6. FIs generally understand and implement their unusual transaction reporting obligations adequately. However, FIU data shows reporting remains low in some sectors. FIs request feedback from the FIU and suggest this is currently inadequate.
7. There are increasing cases of de-risking by FIs and DNFBPs, including of obliged entities. This is worrying and is something the authorities are aware of and should continue to address.

DNFBPs

1. Understanding of risk varies significantly amongst DNFBPs. The land-based casino and TCSPs (trust offices) generally have a good understanding of risks and AML/CFT obligations, but there is a lower level of understanding in other sectors including real estate agents and TCSPs (domicile providers only).

5

2. The implementation of mitigating measures varies across DNFBPs in line with understanding of risks. Trust offices and the land-based casino generally apply mitigating measures commensurate with their risks. Other DNFBPs generally apply CDD measures, but these are often basic and many entities feel CDD is mainly a role for the banks.
3. DNFBPs often struggle to identify the ultimate BOs particularly when this relates to companies with complex structures or entities with an international component and settle for pseudo BOs as an alternative. This is particularly worrying in the case of notaries who often register this information in the BO register.
4. A large number of trust offices use automated screening tools which are effective in identifying possible PEPs. They also show awareness of the EDD measures that need to be taken when PEPs are involved and most have processes to handle customers and transactions from higher-risk countries. Other DNFBPs met during the onsite were aware that specific measures needed to be taken when dealing with PEPs, but, they were often unable to clearly articulate what the specific measures were, that need to be applied in these cases.
5. UTR Reporting in many sectors is low and this seems to be more acute in relation to the legal sector, real estate agents and for sectors where there are no trade organisations (e.g., domicile providers).

BES Islands

1. FIs on the BES Islands have a reasonable understanding of their risks and obligations. Most DNFBPs are not required to identify and assess their ML/TF risk, and the understanding of AML/CFT obligations varies among DNFBPs.
2. Reporting of UTRs is low across many sectors and the process for entities to submit reports appears to be time consuming and overly burdensome.
3. Many DNFBPs rely on screening lists based on open sources and local knowledge. It is very rare that EDD needs to be applied by DNFBPs. On several occasions the Assessment Team heard from the Netherlands authorities and private sector participants that most people on the islands know each other. This may impact the assessment of individual risk.
4. Most FIs and some DNFBPs have a basic AML/CFT policy in place in line with their risks. Training opportunities are limited in the BES Islands and this has impacted understanding of obligations in many sectors.

Recommended Actions

1. The Netherlands should continue to raise awareness of AML risks and obligations, particularly for DNFBPs and smaller FIs and raise TF awareness across all sectors.
2. DNB and AFM should continue to ensure that all FIs are implementing measures commensurate with their risks and address areas of concern, such as a lack of PEP

processes for large parts of the insurance sector and over categorisation of customers as low risk.

3. Obliged entities, in particular notaries, should enhance their efforts to identify the BOs that ultimately have a controlling ownership interest or exercise control through other means of legal entities or arrangements that are part of complex international structures. Obliged entities should also as much as possible limit the identification of natural persons holding senior management positions as BOs. In cases where the ownership structures are so complex or opaque that they pose a genuine ML/TF risk, obliged entities should refuse to provide services.
4. The FIU-NL should improve the feedback and guidance to obliged entities (including those that are not major reporters but are exposed to high ML/TF risks, such as smaller banks, MVTS, VASPs, trust offices, domicile providers, lawyers, and real estate agents) on UTR requirements and on improving the quality of UTRs in order to raise the level of reporting in these sectors, as appropriate.
5. The Netherlands should consider the growing incidences of de-risking and ensure that AML obligations are not being used as a reason to exit particular sectors or groups.
6. The Netherlands (including BES Islands) should require all obliged entities, to take adequate measures to implement TFS without delay and report any actions taken to the competent authorities.
7. The Netherlands should address all technical deficiencies that inhibit effectiveness in the BES islands (e.g., no requirement for obliged entities to assess risk).
8. Options for raising awareness of AML/CFT obligations and providing training for DNFBPs in the BES islands should be considered by the Netherlands authorities.

316. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

Immediate Outcome 4 (Preventive Measures)

317. Considering the relative materiality and risk in the Netherlands, the implementation of preventive measures by the relevant sectors is weighted as follows:

- **Most heavily weighted**: Banking, larger payment service providers and e-money institutions, TCSPs (other than domicile providers), VASPs and the real estate sector (other than real estate agents);
- **Moderately weighted**: Asset management (including includes the broader securities sector and investment management activities), money transfer offices, domicile providers, real estate agents, notaries, lawyers, DPMS, and accountants; and
- **Lower weighted**: Casinos, financial leasing, lending, life insurance and pension funds.

318. As noted in Chapter 1, the banking sector in the Netherlands is highly concentrated with three banks covering over 80% of the retail and commercial market. In terms of asset size, the banking sector accounts for half of the financial sector. The Netherlands has a large, well-developed asset management sector, with approximately 90% of the managed assets of investment firms coming from professional clients, including pension funds. The TCSP sector consists of trust offices and domicile providers. the number of trust offices has reduced substantially since 2018, but the trust office sector is identified as high risk for ML and TF in the Netherlands NRAs, although domicile providers are lower risk and subject to lighter AML/CFT obligations. The volume, speed and cross-border nature of transactions in large payment institutions make them vulnerable for misuse by criminals for ML/TF purposes. Transaction monitoring is a key focus for DNB, which collects transaction data from all MVTS on a quarterly basis. Virtual Assets (VAs) are defined as high risk in the ML NRA. Although VASPs have been recently regulated in the Netherlands, not all VASP activities as defined by the FATF are currently within scope of Dutch legislation. The Netherlands also strengthened its general AML/CFT legislation in 2018, which introduced new obligations for all obliged entities; some smaller obliged entities in certain DNFBP sectors are still adapting to these requirements.

319. The conclusions under IO.4 are based on written documentation (including processes and procedures, case examples and statistics) provided by the Dutch authorities, meetings with DNB, AFM, other supervisors and relevant authorities. The Assessment Team also met with a small number of representatives from relevant sectors and some industry groups. These meetings included small, medium and large banks, which in total represent a significant share of the market in terms of assets, MVTS providers, asset managers, VASPs, lawyers, notaries, accountants, TCSPs (trust offices), real estate agents and casinos.

Understanding of ML/TF risks and AML/CFT obligations

FIs

320. Most FIs in the Netherlands have a good understanding of ML risk, particularly banks, payment service providers and e-money providers. Risk understanding has improved in larger payment institutions following significant efforts by DNB to increase awareness. Understanding of risk in smaller FIs is generally less developed, but adequate.

321. Many of the large banks' risk assessments link to group-wide/global risk assessments, but also include a focus on the specific risks present in the Netherlands. This provides a comprehensive understanding of the local and global risks they are exposed to. In 2019, 85% of all banks and 100% of PSPs completed a Systematic Integrity Risk Analysis (SIRA) according to DNB. A SIRA covers a wide range of integrity risks, such as ML, TF, bribery and corruption, and privacy and data-related breaches. Fifteen percent of the banks had not yet completed a SIRA. This mainly concerned Dutch branches of banks headquartered abroad (EU or non-EU), which rely solely on the risk assessment produced by their head office, rather than having a risk assessment tailored to context of the Netherlands.

322. Most FIs take account of factors such as customer type, products, transaction types and volumes as part of their SIRAs. Banks and large FIs also develop a number of comprehensive scenarios that form their overall risk appetite. Many of the large FIs contributed to the NRA, either directly or through professional bodies, and recognise the risks presented. The NRA is generally seen as a high level policy document. Larger FIs met by the Assessment Team articulated a much more sophisticated view of risk including the types of legal persons and sectors considered as high risk (e.g., professional football clubs and certain types of foundations and church communities). A thematic study of transaction monitoring with a specific focus on TF carried out by DNB in 2018 shows that banks SIRAs contained a limited set of scenarios related to TF. Understanding of TF is generally basic across all regulated sectors in the Netherlands, particularly with regard to transaction monitoring.

Box 5.1. Bank SIRA process involving all lines of the orgnisation

DNB observed how the SIRA process in a bank is the responsibility of all lines within the organisation. At the bank in question, working groups are formed per business unit, in which employees discuss possible ML/TF risks and the likelihood of these risks occurring. The working groups assess, inter alia, the likelihood that certain ML scenarios could allow a customer to launder money through the bank or that international sanctions could be circumvented by the use of the bank's products or activities in certain countries. Using a pre-defined scoring model, the Compliance department, together with Risk Management department, then assesses what the impact would be on the bank if a scenario were to materialise. The sessions lead to a matrix of probability and impact of gross risks. Business departments including the audit and compliance functions then assesses the level of control of the various risks. The matrix of gross risks and control measures then provides an overview of net risks and control gaps.

The result of this exercise is discussed in detail with the management board and it is examined whether the gross and net risks fall within the institution's risk appetite. The management board then decides whether risks should be reduced or avoided and what further measures should be taken.

323. Most FIs have a good understanding of their AML/CFT obligations, although this is lower in the insurance sector, which lags behind other sectors. Risk understanding has improved in recent years. This is due to investigations by DNB, guidance and awareness-raising and high profile failings in two major banks, which led many FIs to reassess their systems and controls. The authorities note that from 2017 onwards, banks have been paying more attention to controlling non-financial risks such as ML/TF risk and these risks are increasingly regarded as an integral part of their overall risk management framework.

5

VASPs

324. Registered VASPs have a good understanding of their risks and obligations. This follows significant interaction and scrutiny over the last year as part of the DNB's registration process. In some cases, policy makers from other parts of the financial sector (e.g., payments institutions) have joined newly registered VASPs in order to strengthen their compliance capabilities. In other cases, DNB has required VASPs to make adjustments to their processes as part of their registration conditions (e.g., to develop more specific risk assessments and for supervisory board members to enhance understanding and risk through training). All VASPs complete SIRAs, drawing on multiple sources, including the NRA, guidance from the supervisor and engagement with the VA trade association.

DNFBPs

325. DNFBP's risk understanding varies depending on sector and size of entity, but is generally basic. All DNFBPs met during the onsite were aware of the NRA and its risks, but some expressed that these risks were not relevant to their businesses.

326. The sole land-based casino and larger trust offices have a good understanding of risk and AML/CFT obligations, but a number of deficiencies have been found in medium and smaller trust offices in recent years. Notaries generally understand their ML obligations, except where it comes to identifying BOs, as they often opt for "pseudo BOs" such as trust offices employees that act as formal directors, instead of taking all necessary steps to identify the ultimate BO. This is particularly the case when offshore and complex legal structures are involved. This is an issue, since the notaries will often register this BO information in the BO register as part of the services they provide to legal persons during their lifecycle (e.g., company formation, change in control). This information can subsequently be used by other obliged entities as part of their CDD processes. Notaries also do not see real estate transactions as a higher risk, despite certain real estate transactions featuring as high risk in the NRAs and referenced during many of the discussions the Assessment Team had with the authorities and private sector.[51] Understanding of risk and AML/CFT obligations in the real estate sector is generally low and many outsource compliance to third parties. Understanding of AML/CFT obligations amongst domicile providers is also low. The authorities have found that some carry out regulated activities that they do not think are regulated and as a result do not apply required AML/CFT mitigating measures. Understanding of risk and obligations amongst lawyers and accountants is generally sufficient and, given the nature of their business, largely relates to offshore businesses and tax crime issues.

327. Supervisors, including professional bodies, have provided guidance to assist their sectors' understanding of ML/TF risks and obligations. However, some smaller DNFBPs do not find this practical. This is problematic for sectors where there are no trade associations (e.g., domicile providers), which often provide additional information and training and is demonstrated in a lack of understanding of AML/CFT obligations.

[51] For example, in its Beleidsregel Integriteitbeleid ten aanzien van zakelijke vastgoedactiviteiten DNB refers to professional real estate transactions as having a high risk of fraud and ML.

BES Islands

328. FIs and the sole trust office on the BES Islands have a basic understanding of risk, which is largely based on the NRAs and guidance provided by the supervisors. FIs and the trust office supervised by DNB understand their obligations and most firms met during the onsite described the generic risks, such as drug and human trafficking, and understood their general obligations. With the exception of trust offices, DNFBPs are exempt from a requirement to take measures to identify and assess ML/TF risks for obliged entities. Notwithstanding, the DNFBPs met by the Assessment Team had a reasonable understanding of generic risks.

Application of risk mitigating measures

FIs

329. FIs met during the onsite have AML programmes and frameworks that are appropriately designed to mitigate ML/TF risks. Interviews during the onsite revealed a strong knowledge of FIs role in the AML/CFT framework and commitment to ensure the financial system is not used to facilitate financial crime. Most large banks have clearly articulated roles for AML/CFT staff, including ownership of AML/CFT risk and issues at board level.

330. Large banks' policies and procedures generally reflect the risks and context of the Netherlands, but only approximately 17% of banks state that their SIRA leads to the formulation of their AML/CFT policies and procedures. This is concerning and suggests a misalignment between the risk understanding and implemented measures. There are increasing examples of de-risking including in relation to VASPs and trust offices. This suggests banks are more inclined to set risk appetites that remove certain groups of customers, rather than implementing mitigating measures in line with the identified risks of individual customers.

331. Almost all FIs have integrated risk mitigation measures into their day-to-day operations and most rely on technology and automated systems that can be adapted easily to emerging risks. Most FIs categorise customers by risk, however the authorities have noted in some cases, customers are categorised as low risk by default, despite having high risk characteristics. Many banks in the Netherlands now refuse large cash deposits, which mitigates risk and also aligns with the profile of the Netherlands, which is one of the most cashless societies in the world.

332. Some of the larger banks have ongoing remediation programmes underway and most of the banks and larger FIs have invested heavily in compliance staff in recent years. Measures to effectively mitigate risks in line with the expectation of the authorities will take some time for banks with large remediation programmes. Large and smaller FIs suggested it is becoming more challenging to recruit appropriately qualified compliance staff in such a competitive environment.

VASPs

333. VASPs are applying mitigating measures commensurate with their risks and the authorities have seen a considerable professionalisation of AML/CFT frameworks during the registration process. Prior to registration, various issues needed to be addressed by many of the firms, including a lack of policies for TFS screening, insufficient risk analyses, wanting to apply simplified CDD with insufficient justification and lack of independent compliance functions. DNB engaged in various outreach activities to help address this and registered VASPs now have stronger measures in place.

DNFBPs

334. Mitigation measures applied by DNFBPs vary considerably. Some larger international DNFBPs (e.g., auditing and accounting firms) implement a sophisticated risk-based approach, and assess risk-based on factors such as the client's country, whether the client is a PEP, etc., and classify customers in order to conduct CDD in accordance with risks. Smaller DNFBPs apply basic CDD measures and are much less risk-based. Often CDD is limited to identifying and verifying documents at the customer acceptance stage.

335. Most licensed trust offices have policies and procedures in place that are designed to mitigate ML/TF risks. In some cases these are insufficient to effectively mitigate and manage potential integrity risks.

336. The one casino in the Netherlands takes robust risk-based mitigation measures. These include comprehensive identity verification checks at the customer registration stage, transaction limits for newly registered customers and large-scale monitoring systems. Online casinos recently became subject to AML/CFT obligations through the Remote Gambling Act (October 2021) and there is no information at this stage on the extent that they are implementing these obligations.

337. The NOvA and other professional bodies provide training, including on AML/CFT. Most law firms that carry out Wwft activities have an office policy and approximately 44% have a compliance officer. Notaries generally implement mitigating measures, although they believe they are more limited in terms of when they can refuse customers, because of their statutory obligation to provide services.

338. Many other DNFBPs do not have appropriate risk policies and procedures in place. In response, several supervisors produce risk policies and templates to assist institutions fulfil this obligation.

339. The authorities invest significantly in providing guidance to mitigate risks and many private sector participants referred to the ability to contact the authorities with questions. Several authorities have dedicated helpdesks for this purpose and the smaller DNFBPs see this as a useful source of information and advice. As with the banking sector, there are signs of de-risking amongst DNFBPs.

BES Islands

340. FIs in the BES Islands categorise their customers based on risk; however, they often fail to fully acknowledge relevant risks as articulated in the NRAs and focus on their Wwft BES obligations. As a result, the inherent ML/TF risks will not be properly addressed by internal control measures. Generally, most FIs and trust offices on the BES Islands conduct entity-level risk assessments, but have a challenge when it comes to applying a risk-based approach on customer level, which tends to result in over compliance. DNFBPs except for trust offices are not required to take measures to identify and assess ML and TF risks. Notwithstanding this, some DNFBPs met by the Assessment Team had undertaken a risk assessment.

Application of CDD and record-keeping requirements

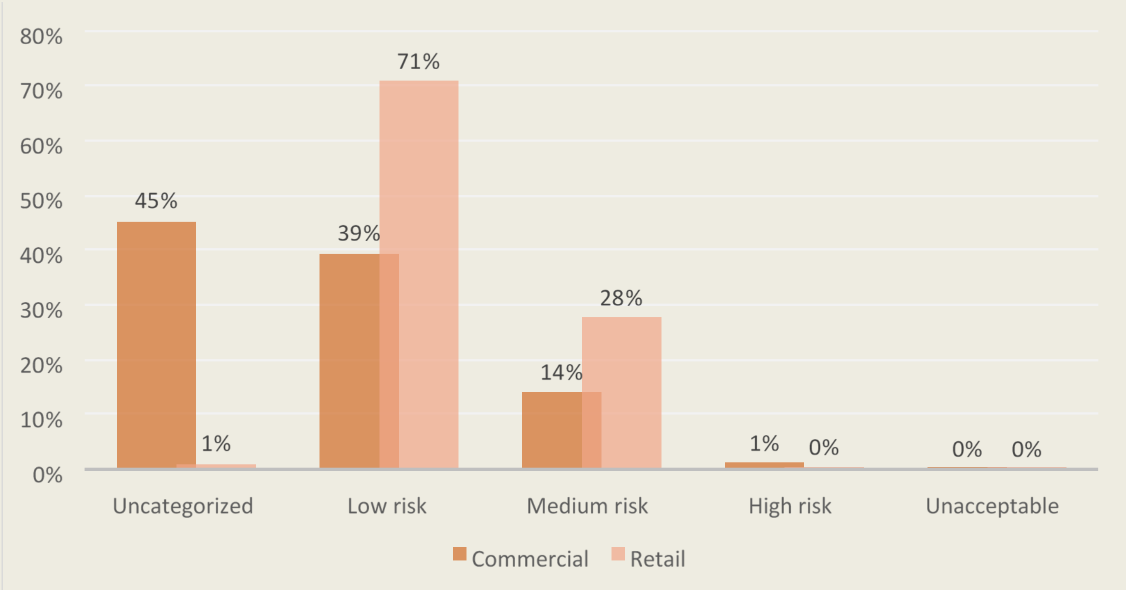
341. Interviews with all FIs suggested that they understand their CDD obligations. There was a mixed understanding in relation to record keeping requirements, with some FIs stating they kept records longer than required, and often the DNB finds that some BO information is missing.

342. FIs have effective processes in place for onboarding customers and carrying out CDD, including online only banks. However, some FIs including banks generally struggle to identify BO information, particularly when complex international structures are involved. The AFM finds that in a number of investigations with customers who have complex legal structures, FIs regularly fail to identify and verify the BO and DNB finds that in practice banks find it hard to (fully) comply with identifying and verifying BOs in certain cases.

343. Much of the onboarding process is done electronically for standard customers, but handled manually in cases were certain flags are raised (i.e., a non-standard customer). DNB noted that some banks and PSPs had procedures where customers were almost all placed in the low-risk category by default. This has led to inappropriate CDD measures being applied, including transaction monitoring. Furthermore, DNB has found that in some institutions, customers that are identified as low risk for ML are automatically categorised as low TF risk with no TF analysis being carried out. As part of their remediation programmes, several banks are now reviewing their legacy customers to ensure they are appropriately categorised and subject to commensurate CDD measures. This is a significant undertaking and in some cases leads to the retrospective submission of a number of UTRs. The below chart summarises the percentage of banks that establish a risk profile for their customers prior to providing services.

5

Box 5.2. Percentage of banks that establish a risk category or profile for customers prior to providing services (2019)



344. DNB has found similar results for PSPs in terms of categorising customers as low risk. Furthermore, in response to the annual risk questionnaire, only 8% of PSPs indicate that they have a risk appetite with verifiable indicators and/or limit values. PSPs appear to be aware of their exposure to TF and DNB has noticed that MTOs are increasingly paying attention to certain customer groups, such as charity foundations and foundations with a religious background. This is in line with the TF risks identified in the TF NRAs.

345. FIs met by the Assessment Team exit customers when there is reason to do so, but this is rare. Exit records are often not maintained or do not clearly demonstrate why the customer was exited. One bank explained that it was very challenging to exit customers and described how a court had intervened when they tried to exit a customer that would not provide additional information. This type of intervention may increase banks' reluctance to accept certain groups of customers on a wholesale basis.

VASPs

346. VASPs met by the Assessment Team explained their CDD processes and record keeping obligations. All used blockchain analytics software to monitor and analyse ongoing customer transactions and some take a risk-based approach in terms of applying transaction limits on new customers. Corporate customers generally have to provide source of wealth, UBO information, structural information and explain the purpose of account. All VASPs met during the onsite had robust record keeping processes in place.

DNFBP

347. The majority of trust offices categorise customers based on risk and have risk appetites in place. Customer files are reviewed on an ongoing basis and since a change to the regulations in 2018, customer files are supplemented with more in depth risk-related information. However, DNB still finds examples of incomplete CDD files in trust offices. For example, when accepting a customer, the trust office must describe the integrity risks associated with the provision of services and the extent to which they are mitigated in conjunction with each other. Often these descriptions are not complete as it is a fairly new requirement. The land-based casino has strong CDD measures in place and records are maintained on all customers. Individuals who fail to provide appropriate CDD information are banned from the casino and customers exited for CDD failings are reported to the FIU-NL.

348. With the exception of trust offices and land-based casinos, most DNFBPs understand CDD as identifying the customer and checking the presence of documents. Most of these DNFBPs assume that banks' CDD processes are more advanced and the CDD the DNFBPs do duplicates that of the banks. Real estate agents often outsource their CDD requirements and appear to have little understanding of what this fully entails, despite being ultimately responsible for the process. Most DNFBPs struggle to identify BOs and in some cases too often only identify pseudo BOs, which is particularly troublesome in the case of notaries. Notaries, lawyers and accountants met during the onsite all described compliant CDD processes. All DNFBPs met during the onsite understand their record keeping obligations but there were different responses regarding how long records needed to be kept for. Furthermore, BFT has found that correct data is not always recorded. CDD failings found by the authorities are summarised below. The failings for domicile providers are consistently high, which is a concern given their role in the TCSP sector.

Table 5.1. Number of CDD shortcomings detected per sector

DNFBPs	2016	2017	2018	2019
Casino[52]	-	-	-	-
Real Estate Agents	302	220	127	107
DPMS	6	7	16	79
Lawyers	1	2	8	9
Notaries	8	9	9	7
Accountants	5	2	2	4
Trust Offices	26	23	16	15
Domicile Providers	16	15	28	2
Total	364	278	206	144

349. Many DNFBPs met during the onsite explained processes for exiting customers, but very few could provide examples where this had been done in practice. Where customers had been refused it was usually for lack of information. Notaries are subject to a ministerial duty and can only refuse to provide services in certain specific cases, for example, where it is clear there is a frontman or sham structure. This is a concern given the role notaries play in real estate transactions and company formation.

BES Islands

350. The Assessment Team met one FI that explained their CDD processes and record keeping requirements. The authorities suggest that CDD processes within banks are generally based on the standards deployed by their internationally operating mother companies. Smaller credit institutions have difficulties when it comes to well-qualified staff, resulting in (sometimes less than) basic CDD processes. Life insurance companies have CDD processes in place commensurate to their risk profile.

351. In terms of DNFBPs, most CDD omissions in the BES Islands concern incomplete data on natural persons. Omissions relating to incomplete BO information for real estate agent customers are found sporadically by the BTWwft. This is a significant concern given the risk of ML in this sector.

[52] Data for shortcomings by casinos is not available.

Application of EDD measures

FIs

352. Implementation of EDD measures varies amongst FIs, depending on their size and international exposure, but is generally done well. Most FIs have formulated policies and measures for entering or continuing a business relationship with a PEP and this includes automated screening systems, which screen on a regular, if not daily basis. DNB's annual questionnaire shows that 66% of banks have specific business rules for PEPs in regard to transaction monitoring. AFM has found that investment institutions formulated too few concrete processes for PEPs, although in practice they generally complied with obligations to identify them. They also found that only approximately half of insurance intermediaries have procedures to determine if a customer is a PEP, which is low given the longstanding requirement for them to do so. DNB has found that PSPs often still need to outline what concrete steps need to be taken to manage PEP relationships.

353. DNB carried out a thematic review between 2015 and 2017, focussing on correspondent banking. This review found that most banks were not sufficiently complying with their obligations. Since the thematic review, DNB has noted that banks increasingly recognise the risks of correspondent banking, are drawing up a risk appetite and taking the necessary control measures to mitigate the risks. Banks met by the Assessment Team noted that in many cases they had reviewed correspondent banking relationships in recent years and terminated some of these, particularly in higher risk jurisdictions.

354. Many FIs are using new technologies and this appears to have increased during the COVID-19 pandemic, particularly for onboarding. Several FIs referred to measures they were piloting or implementing in terms of artificial intelligence and machine learning. In these cases, robust risk analyses were performed and any pilots were operating alongside existing systems. One of the FIs expressed frustration that they could not get a view from the authorities on whether specific systems would be in line with supervisory expectations and were concerned that they were investing resources to improve effectiveness, without confidence they would meet the expectations of the authorities.

355. FIs in the Netherlands are subject to the EU wire transfer regulations and have established systems in place to comply with these regulations. The annual integrity risk questionnaire shows that 51% of banks monitor transactions based on transaction characteristics and 23% of banks refused transactions due to insufficient information from either the payer or the payee. FIs in the Netherlands use a range of automated systems and vendor services to monitor the various TFS lists. DNB notes that banks generally carry out this screening and report any match to the relevant bodies. This is not always the case with PSPs, and some small scale MTOs manually screen lists. Branches of insurers (life and non-life) operating in the Netherlands by means of a notification must also screen their relations against the National Terrorism List and the EU lists and DNB believe they are largely compliant with this. FIs apply EDD in the case of customers or transactions in higher risk countries and often use sources such as the Transparency International Corruption Index.

356. Banks use various lists and sources to identify and maintain their understanding of high risk countries and integrate this into their customer acceptance and ongoing CDD processes. MVTS providers generally use the FATF list of high-risk and other monitored jurisdictions and have appropriate controls in place. This is important particularly as a small number of MVTS providers make and receive payments from higher-risk jurisdictions. Other FIs consult lists provided by the authorities, as well as the FATF, and many have automated processes to flag customers and transactions from high-risk jurisdictions.

VASPs

357. VASPs interviewed implemented some EDD measures, including PEP screening, request more information from higher risk customers and monitor customers and transactions against TFS lists.

DNFBPs

358. Trust offices generally apply EDD measures effectively. DNB finds that in some cases of PEP exposure, the BO is checked without identifying and verifying all 'relationships' that might be PEPs. Automated systems are used for TFS screening and automated transaction monitoring is increasingly being used. DNB's 2019 annual survey found that 56 trust offices operated target companies in sanctioned countries and often the risks of TFS are insufficiently described in risk assessments. EDD measures for customers in higher risk countries are generally robust and involve things such as considering the purpose of the transaction. However, notaries carrying out transactions to high-risk countries on behalf of their clients, are not able to disclose information on the customers to the FIs because of professional secrecy. This is an issue that is currently being considered at the ministerial level as some banks have threatened to close notary third party accounts in cases where they are unable to fulfil EDD requirements.

359. The land-based casino applies EDD measures to PEPs and customers from high risk countries. Most DNFBPs met during the onsite had very few PEP customers, but were able to explain measures taken to identify and apply mitigating measures, which largely relates to requiring senior management agreement to take on the client. Smaller obliged entities in other sectors, including lawyers, notaries and real estate agents often ask customers to self-declare if they are PEPs, rather than automatically screening names against lists. It is not clear the extent to which the self-declarations are scrutinised to determine if the declarations are accurate. There was also general knowledge in terms of requirements for clients from high-risk countries, but it is unclear how well measures are applied in practice and the authorities do not have a strong view on this. This is a concern, particularly in relation to domicile providers as many of their customers are from other countries, making it more difficult to identify PEPs. As previously mentioned, most real estate agents outsource compliance but gave examples during the onsite of where high-risk situations had led them to take additional measures, including forgoing sales.

360. Casinos, real estate agents, DPMS and legal professionals (those who are not also providing services as a trust office) are exempted from the obligation to report frozen assets under TFS to a supervisory authority. The Netherlands states that this exemption is based on the TF NRAs as there are no TF risks identified in these sectors. The Assessment Team does not consider these exemptions as risk-based, as the implementation of TFS is not a risk-based requirement and all relevant requirements should apply equally to all obliged entities (i.e., it is a rules-based requirement). Accordingly, the Assessment Team considers this a deficiency that impacts effectiveness.

BES Islands

361. Banks in the BES Islands generally follow the same processes as banks in continental Netherlands in relation to PEPs, correspondent banking and TFS monitoring. This includes using automated customer screening and transaction monitoring software. Some FIs make use of PEP lists they have drawn up themselves, or rely on the local knowledge of their staff with open source checks. DNFBPs met by the Assessment Team were able to describe processes for identifying PEPs and identifying customers from high risk countries. During onsite interviews, the Assessment Team regularly heard that everyone in the BES Islands know each other and this was why certain EDD obligations were not always fulfilled. With the exception of trust offices, DNFBPs and VASPs implementation of TFS without delay is not supervised.

Reporting obligations and tipping off

362. Obliged entities must submit objective and subjective UTRs (see IO.6). Compliance with reporting requirements is heavily monitored and appears to be a significant focus for most supervisors. Overall, firms met by the Assessment Team understood and implement their reporting obligations adequately. However, it is not clear this applies equally across all sectors, as UTR filing is low by some DNFBPs such as lawyers.

Table 5.2. Submitted UTRs by obliged entities

Type of obliged entities	2016	2017	2018	2019	2020	2021*
Auditors	1 260	1 155	1 879	2 502	2 466	2 453
Lawyers	12	10	21	42	21	12
Banks	13 599	22 789	67 524	147 952	245 148	227 025
Investment institution/companies	4	6	59	69	273	214
Life insurance brokers	0	0	1	0	0	4
Money transfer offices	36 0234	279 950	248 630	199 199	194 894	239 946
Payment service providers - PSPs	12 315	29 669	42 959	151 576	227 987	335 134
Dealers in Precious stones	396	471	502	729	726	710
Undertakings for Collective Investment in Transferable Securities	0	0	0	0	3	7
Life insurers	2	3	1	5	9	17
Real estate agents	140	159	169	221	246	196
Civil-law notaries	529	486	784	1 285	1 060	964
Gambling casinos	2 666	3 228	4 110	4 724	3 764	2 949
Providers of remote gaming services	n/a	n/a	n/a	n/a	n/a	233
Trust and company service providers	0	240	206	192	146	78

Safe custody services	0	0	0	0	52	30
Providers of services for the exchange between virtual currencies and fiduciary currencies	280	0	0	0	7 066	171 958
Providers of custodian wallets	n/a	n/a	n/a	n/a	243	101 427
Exchange institutions	0	3	360	562	491	353

*Covers the period up to November 2021.

FIs

363. FIs are aware of their responsibilities to report UTRs. In general, reporting has increased since 2017, and this is particularly the case for FIs supervised by the AFM (see Table 5.2). The AFM believes this is partly due to legislation, but also increased awareness of obligations across the sector.

364. Foreign banks based in the Netherlands are sometimes confused by the difference between UTRs and STRs as they operate based on procedures from their parent companies. DNB notes that some banks do not report transactions that are rejected (for both incoming and outgoing transactions). Most FIs automate the UTR objective indicators, which mainly relate to transactions over certain monetary amounts. Many banks are improving transaction monitoring as a way to improve the efficiency and are submitting a significant number of UTRs from historic transactions as part of remediation exercises (see IO.1 for a case study related to a private-private sector initiative to better identify UTRs).

365. The quality of transaction monitoring systems and business rules is still insufficient to recognise all the subjective unusual transactions for some MVTS providers. This is an area of focus for DNB, which has seen improvements in transaction monitoring of subjective indicators since providing guidance in 2017 and 2018, and as a result of its investigations.

366. All FIs appear to be aware of their tipping-off obligations. In banks and large PSPs, reporting is done by compliance departments, which adds as an additional protection as there is little involvement of front line staff once the initial reporting query has been raised.

367. Many banks met during the onsite expressed concerns that despite the increased focus on reporting and the fact they are submitting more UTRs, they see few tangible results in terms of reducing crime, feel that only a small number of reports are disseminated to LEAs (see Table 3.1) and they do not receive feedback from FIU-NL.

VASPs

368. VASPs are aware of their requirements to submit UTRs and tipping-off obligations. Reporting has been a key area of focus of DNB and they have noticed a large spike in UTR numbers following thematic work in this area. One VASP felt the requirement to file objective UTRs (i.e., threshold reporting) for transactions over EUR 15 000 was too low given their typical customer activity. This is concerning given the risks associated with VASPs, which are set out in the NRAs. This view was not echoed by any other obliged entity.

DNFBPs

369. Trust offices met during the onsite are aware of their reporting obligations and submit UTRs. The number of UTRs submitted by the sector has increased in recent years and obliged entities explained that UTR submission was a key focus of DNB. The quality of reporting across the trust office sector varies and sometimes the level of detail in reports is insufficient. As with FIs, DNB finds that responsibility for reporting in trust offices is often allocated to the compliance department and is therefore separate from the account managers who have contacts with customers. This significantly reduces tipping-off risks and trust offices met during the onsite were all aware of their responsibilities in this regard.

370. Reporting by other DNFBPs has also increased in recent years, but is still not sufficient compared to the size of the sectors. Most DNFBPs met during the onsite submitted an UTR, but in one case a real estate agent had paid his compliance company to submit one on his behalf. This practice is concerning to the Assessment Team as agents may be influenced in their decision to submit an STR because of the cost incurred for each UTR. Notwithstanding, the authorities note that developments in the commercial real estate sector are positive. The supervisors note that there are relatively few problems in terms of objective UTRs, but a lack of knowledge and expertise on ML and TF makes it hard for some obliged entities to file subjective UTRs. Very few UTRs have been submitted by lawyers. In 2019, only 22 firms from more than 5 000 had submitted a UTR. This figure appears low for the size and risk profile of the sector. The authorities explain this is due to the fact that only a small number of lawyers carry out activity subject to AML/CFT regulation. Most obliged entities could explain tipping-off requirements to a basic extent.

BES Islands

371. Most UTRs in the BES Islands are submitted by FIs. The large FI met by the Assessment Team submitted approximately 500 UTRs per year. All obliged entities from the BES Islands met during the onsite were able to explain the process for submitting UTRs and their tipping-off obligations. Unlike in the Netherlands, UTRs must be submitted manually and it was felt that this process was very time consuming (up to three hours per UTR), and may deter reporting.

5

Table 5.3. Submitted UTRs by obliged entities in BES Islands

Type of obliged entities	2016	2017	2018	2019	2020	2021*
Auditors		2	1	2	0	0
Lawyers		0	2	0	0	0
Banks	1 109	974	905	931	701	1 593
Payment service providers		1	0	0	0	0
Customs	121	41	46	25	97	35
Dealers in precious stones	2	4	4	18	6	9
Real estate agents	5	1	2	0	1	0
Civil-law notaries	30	8	21	23	22	24
Gambling casino		0	2	1	0	2
Total	1 287	1 031	98	1 000	827	1 663

*Covers the period up to November 2021.

Internal controls and procedures

FIs

372. Banks and other large FIs interviewed by the Assessment Team demonstrated a positive AML/CFT compliance culture, primarily driven by recent large settlements for major banks and reputational concerns. DNB has observed a greater understanding of AML/CFT compliance at the senior and board level in larger FIs. Some of the banks met by the Assessment Team use external parties for auditing and there are doubts about their independence and quality of work. The same applies to PSPs. Furthermore, DNB observes that the second-line and third-line functions in insurers often still fulfil their monitoring role insufficiently. All FIs met during the onsite provide comprehensive training to staff on AML/CFT measures. Dutch and foreign MVTSs operating in the Netherlands have training programmes for their employees and agents. Most FIs screen their employees and the extent depends on the position in question and often includes requiring a certificate of good conduct. Several of the large banks are part of financial groups and put in place or follow global standards and do not find any issues in relation to sharing of information within the group. DNB and AFM have not been informed of situations where difficulties have arisen, but are in discussions with some institutions about sharing suspicious transaction information within the group where they encounter conflicting local legislation in other EU member states.

VASPs

373. VASPs met during the onsite had robust controls and processes in place, commensurate with their size. Some had hired compliance professionals from the financial sector and commissioned external partners to deliver specific compliance training. Process manuals were in place and scrutinised by DNB as part of the application process. One of the VASPs met felt there was a risk in some firms that the compliance function did not keep up with growth of businesses. This is something DNB will need to keep under review in the future, particularly as there is increasing competition for compliance staff across the financial sector.

DNFBPs

374. Governance requirements were tightened for trust offices in 2018 and include a requirement to have independent compliance and audit functions and separate board members responsible for each. Most trust offices outsource this function to external parties. The trust office sector professional body Holland Quaestor (HQ) provides training for trust offices and requires its members to undergo a certain amount of training each year. Only 16 trust offices are members of HQ, but these are mainly the larger trust offices and according to HQ data account for 70% of the commercial market share. Most trust offices have a procedures manual, which is also a requirement under the Wtt 2018, but DNB finds these do not always adequately identify all integrity risks or include appropriate control measures.

375. The land-based casino has robust policies and procedures that are well documented. Staff undergo training, including how to recognise suspicious behaviour. Notary offices are peer reviewed once every three years, covering all civil notary requirements including AML/CFT controls and processes. Some notaries have policies and procedures in place according to the BFT, but the level of implementation of policies and controls is unclear. Accountants are also peer reviewed and findings tend to be similar. Larger institutions under BTWwft supervision have manuals, regulations or internal programmes which enable staff to be alert to the obligations arising from the Wwft.

376. Medium and larger sized law firms met during the onsite had compliance functions within their organisations. Often these firms provided several services, including notarial services and the compliance department covered all areas. These firms were also subject to external auditing and had ongoing training for staff. Smaller obliged entities in sectors such as real estate, accountancy and DPMS have basic manuals or internal programmes depending on their size, but not all have compliance arrangements in place. The authorities did not provide sufficient information to determine how well all DNFBPs are applying internal controls and procedures.

5

BES Islands

377. FIs in the BES Islands generally have compliance function and audit arrangements, despite challenges with attracting appropriately skilled staff. Audits are generally carried out by the parent company's internal audit company once every 2-3 years. There are some cases where compliance officers are located away from branches. Many FIs have training programmes and some use third parties to deliver this online. With regards to DNFBPs, available training is not always appropriate and does not specifically cover BTWwft requirements. DNFBPs do not generally attend training and there is no training provider in the BES Islands for DNFBPs. Until recently, civil-notaries did not have to share files for review by the supervisor. This is a concern given their role in real estate on the islands.

Overall conclusions on IO.4

1. Understanding of AML/CFT risks and obligations varies across FIs and DNFBPs. This is generally high for banks, larger FIs and VASPs, but lower for DNFBPs, particularly domicile providers and real estate agents. Understanding of TF risks is lower across all sectors.
2. Implementation of mitigation measures varies across sectors. They are generally stronger in larger banks and FIs that have automated systems, governance processes and three lines of defence models. Mitigating measures are weaker in most DNFBPs, particularly in some higher risk areas such as the provision of TCSP activities.
3. Identifying BO remains difficult for many obliged entities, including larger FIs. This regularly leads to pseudo BOs being identified, particularly by notaries. EDD measures are usually applied, although it is concerning that in the insurance intermediary sector only half of obliged entities have systems to identify PEPs and a significant number of PSPs have not identified concrete steps to deal with PEPs. Notaries do not provide FIs with information on clients they are performing transactions on behalf of because of professional secrecy.
4. Although customers' screening against international TFS lists is not a requirement stemming from the FATF Standards, those DNFBPs with automated processes tend to do this as a matter of course. Obliged entities are generally aware of their reporting and tipping-off obligations. Reporting in some sectors remains low and some FIs requested more feedback from FIU-NL on the UTRs they are submitting. There is some concern that despite submitting an increasing number of UTRs, they do not see this corresponding to significant outcomes.
5. The Netherlands is rated as having a moderate level of effectiveness for IO.4.

Chapter 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

FIs and VASPs

1. The Netherlands has a strong licensing framework to ensure criminals and their associates are not beneficial owners or hold controlling interests in FIs. A robust set of checks exist to ensure persons holding key functions are fit and proper. Individuals are reassessed, as appropriate, and action is taken to remove individuals from management positions when necessary. A robust registration process also exists for some VASPs, but not all VASP activities in the Netherlands are subject to registration and supervision.
2. The Netherlands recognises the existence of underground banking through unlicensed payment services and hawala networks, but does not currently allocate sufficient supervisory resources to address this.
3. DNB and AFM have a good understanding of ML/TF risk, which is increasingly data driven and supported by a comprehensive risk analysis questionnaire that all obliged entities must complete on an annual basis.
4. DNB and AFM apply risk-based supervision and, DNB in particular, has been innovative with the use of data and technology in order to deliver more effective supervision. This has accelerated during the COVID-19 pandemic. However, the frequency of supervision in some cases is low.
5. The Netherlands has a range of enforcement measures and DNB and AFM are able to impose fines of up to 20% of a FI's annual turnover in the most serious cases. DNB and BFT have imposed more formal measures than informal measures for AML/CFT breaches; however, other supervisors rely heavily on informal measures, which are not published. In the few cases where significant settlement cases were concluded and published, this resulted in a deterrent effect across the industry.
6. The Dutch authorities generally require remediation plans to be put in place in all cases where they find AML/CFT deficiencies. These are followed up, even when they are imposed with informal measures. This allows the authorities to ensure actions are being remedied.
7. All supervisors produce a range of guidance and invest significantly in outreach with supervised sectors. However, several private sector representatives suggested that some of the guidance is better suited for large institutions and could be more specific.

6

DNFBPs

1. With the exception of trust offices and casinos, there is no legal requirement for DNFBPs in the Netherlands to be licenced or registered for AML/CFT purposes. Lawyers must become members of the Netherlands Bar. Notaries are appointed by the authorities and both notaries and accountants are required to be members of professional bodies.
2. Despite illegal trust activity in the Netherlands being identified as high risk, there has been little enforcement action in this area and insufficient resources are currently allocated to address this issue.
3. Understanding of sector risk by DNFBP supervisors varies. Understanding of individual trust offices is strong and DNB risk profiles these entities in a similar way to FIs. The BTWwft has sector coordinators, which produce sector descriptions listing the ML/TF risks in the sectors it supervises. BFT supplements its understanding of risk through engagement with professional bodies.
4. Most DNFBP supervisors do not apply an appropriate frequency and intensity to their supervision programmes. Although efforts are being made to better develop risk-based approaches, supervision is generally carried out on a reactive basis.
5. Professional bodies in some sectors carry out peer reviews in agreement with the supervisor. Where incidences of AML/CFT failures are found during peer reviews, they can be escalated to the BFT and can lead to formal and disciplinary measures. However, the number of escalations is low and does not appear in line with the obliged entities' level of understanding and levels of compliance with their AML/CFT obligations.
6. With the exception of trust offices, DNFBPs implementation of TFS without delay is not supervised. The same deficiency applies to DNFBPs and VASPs in the BES Islands.
7. Some DNFBP supervisors rely heavily on warning letters and other informal measures, including where unlicensed activity is identified. In such cases, it can take more than a year for cases to escalate to formal action to prevent them from continuing to operate.

BES Islands

1. There are no entry controls for VASPs in the BES Islands and the authorities do not know of any operators located on the islands. There are also no entry control requirements for DNFBPs in the BES Islands.
2. Understanding of risk in the BES Islands is generally good and this is made easier by the small number of entities in the jurisdiction.
3. Supervision is usually done in blocks of 2-3 weeks annually. There is generally good coverage of the population and DNB's last supervisory visit to the islands was in October 2021. However, the BTWwft has never reviewed the files of the island's civil law notaries, since they did not have the legal powers to do this until 1 July 2021. This is a concern given the role of notaries in the high risk real estate sector. BTWwft plans to review these files in 2022.

Recommended Actions

1. The Netherlands should extend licensing or registration and supervision to all VASP activities covered by the FATF Standards.
2. The Netherlands should strengthen measures, including increasing resources, to tackle unlicensed activity, including underground banking and the provision of illegal trust offices.
3. The Netherlands should ensure that all DNFBP supervisors have robust measures in place to ensure that they are able to identify criminals and their associates and prevent them from owning or controlling legal entities in the regulated sectors.
4. The Netherlands should consider additional legislation and other measures to reduce the ability of companies providing TCSP services to restructure their operations in order to circumvent stricter regulation.
5. The Netherlands should improve its understanding of risks in all DNFBP sectors in order for resources to be allocated appropriately and ensure effective risk based supervision.
6. The Netherlands should assess the effectiveness of peer review supervision, to determine whether findings align with the ML/TF risk profile of the sectors they supervise.
7. The Netherlands should ensure that appropriate resources are available to all supervisory authorities, so that they can conduct risk-based supervision with varying levels of intensity. AFM and DNB should consider if all firms they supervise are subject to appropriate frequency of supervision.
8. Supervisory authorities should ensure that obliged entities fully comply with their obligations to identify BOs in legal persons or other arrangements that are part of complex international structures in order to limit the identification of senior officials as pseudo BOs to a minimum.
9. Supervisory authorities should make full use of the powers available to them, tailored to each specific case, and rely less on informal measures when significant AML/CFT violations are identified. All DNFBP supervisors should ensure they have appropriate enforcement policies so there is clarity when specific interventions should be applied.
10. The BTWwft should subject the notaries on the BES Islands to appropriate supervision as a priority.
11. The Netherlands should require all obliged entities to take adequate measures to implement TFS without delay and ensure supervisors monitor compliance with this requirement in their respective sectors. The authorities should maintain statistics on the extent obliged entities adequately freeze and report frozen funds or assets from designated individual or entity without delay.
12. The Netherlands should continue to produce high quality guidance and ensure this is relevant for smaller entities. This guidance should cover areas where there are identified gaps in knowledge, including in terms of understanding of ongoing CDD measures.

378. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

379. The weighting given to the different financial and DNFBP and VASP sectors regarding supervision is the same as applied for preventive measures (see IO.4 and Chapter 1 for further details).

380. The conclusions in IO.3 are based on: statistics and examples of supervisory activities and actions provided by the Netherlands; guidelines and guidance issued by the supervisors, documents used to monitor the different reporting sectors; discussions with the DNB, the AFM, DNFBP supervisors, as well as representatives of a broad sample of FIs, DNFBPs and VASPs (including from the BES Islands).

381. The Netherlands has several authorities responsible for supervision of FIs, VASPs and DNFBPs. The relevant supervisors are summarised in Tables 1.3 and 1.4 in Chapter 1. The Assessment Team focussed most heavily on measures for the supervision of banking, MVTS and trust offices, given their materiality and risk in the Netherlands. VASP supervision is at an early stage in the Netherlands and it is a relatively small but growing sector. With this in mind, the Assessment Team focused significantly on the licensing activities and early stages of supervision. Real estate, payment services and the legal and accounting sector were also an area of significant focus given their key gatekeeping role. Pensions, life insurance and many of the activities supervised by the AFM are lower risk. The same applies to the casino sector and appropriate weighting was given to these activities. The Netherlands also supervises for AML purposes activities that are not within the scope of the FATF standards (e.g., tax advisors, dealers in vessels, kitchen and bathroom dealers and car dealers). These sectors were not considered as part of the evaluation.

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

FIs

382. The Netherlands has a robust legal framework for the licensing of FIs. All FIs must be licenced by DNB, AFM or the European Central Bank (ECB) before they can operate in the Netherlands. DNB also supervises a small number of firms that are exempt from licensing and registration requirements (e.g., advice on capital structures, financial leasing, commercial lending and safe custody).

383. Depending on the type of institution, a legal person is assessed for licensing by DNB and/or the AFM. Both authorities work together on joint assessments, follow the same process and use the same substantive criteria. All FIs operating in the Netherlands must have a physical presence and must be registered with the CoC, unless they are from another EU member state operating under passporting arrangements.

384. Licensing processes for FIs include comprehensive fitness and propriety checks for policymakers (including supervisory and executive board members) and key function holders. Criminal records are obtained through the OM and where there is an indication that the applicant has a relevant criminal background, or is associated with criminals, additional checks are carried out. This involves searching open source information, as well as consulting iCOV. Applications are submitted through the Digital Supervision Portal and approximately 25% of applicants are interviewed by DNB as part of this process. AFM conducts a small number of interviews as part of the application process including for insurance intermediaries, which self-declare that they meet AML/CFT requirements. In 2021, approximately 13% of applicants in the investment firm and investment institutions sector were subject to interviews. The number of interviews carried out by AFM as part of licensing appears low, despite the sectors being lower risk than some other FI sectors.

385. Controllers are subject to reputation assessments (fit and proper tests) and must obtain a declaration of no objection from supervisors before they can hold a controlling interest in an obliged entity. The same applies when an applicant for a qualifying holding is a legal person. Reputation assessments apply to those with a direct or indirect holding of at least 10% of the issued share capital, or the ability to exercise, directly or indirectly, at least 10% of the voting rights or of comparable control. The authorities also require FIs to declare all BOs that hold a 1% interest or more or 0.5% where the FI is a credit institution. In certain higher risk cases, the authorities ask for details on holders of less than 0.5% and do so in all cases where a fund structure has a holding interest. Where the BO holds a controlling interest and is located in another jurisdiction, supervisors require a certificate from a CoC and criminal records checks of the policymakers of the BO from their home authorities.

Table 6.1. Natural persons assessed by DNB, per sector

Sector	2016	2017	2018	2019	2020	2021*
DNB						
Payment institutions, including currency exchange offices	88	105	41	347	275	124
Credit institutions*, including branches located in the Union	258	169	98	280	203	74
Credit institutions - second level	71	56	43	51	49	21
Insurance undertakings	208	196	183	303	342	91
Insurance undertakings - second level	72	49	40	31	33	9
Pension funds	472	427	410	557	713	206
Trust offices	144	99	135	179	170	103
VASPs	-	-	-	-	110	70
AFM[53]						
Life insurance intermediaries *[excluding banks and insurers[54]]*	838	1 023	915	827	955	932
Investment firms	211	102	105	190	260	251
Investment institutions	0	3	17	2	6	4

*Covers the period up to June 2021

53 AFM carries out fitness and priority checks separately.

54 Under the Wfm BES, DNB issues licences to these FIs and conducts assessments of persons.

386. Approximately 5% of applicants are not fit and proper, but some applicants withdraw their application during the process where additional information is requested and where it becomes clear that the supervisor has concerns. The figures for AFM are slightly lower. The below case study summarises an instance where a license application was withdrawn.

Box 6.1. Licence application withdrawn

In 2018, DNB received an application for a licence to provide payment services. The party concerned wished to act as an online money transaction office. The institution proposed two directors, which were subject to an assessment. During the preliminary investigation it was discovered that one of the proposed directors was involved with companies related to so-called Ponzi schemes. DNB made further inquiries via the FEC about any other signs of involvement with financial and economic crime. In addition, a report providing an overview of the equity and income of the directors was requested via the Information Exchange on Criminal and Unexplained Wealth (iCOV). The Police and FIU-NL (on the basis of the request made via the FEC) shared relevant information on both directors at the request of the DNB and an iCOV report provided an overview of a criminal network.

During the assessment interviews with the directors, one proposed director stepped down. The institution continued the licence application process by proposing another director. When it became apparent that DNB intended to issue a negative decision concerning the newly proposed director - primarily because of his fitness - the institution's board decided to withdraw the licence application in full. Consequently, the payment service provider did not enter the Dutch financial market.

387. The fitness and propriety of individuals is reassessed when there are material changes, including adverse media reports calling into question the suitability of individuals. For example, DNB carried out 10 reassessments in 2019 and AFM completed seven.

388. The Netherlands recognises underground banking through unlicensed payment services as presenting a high ML/TF risk. Hawala networks were noted in several discussions with the authorities and the private sector during the onsite visit. The authorities receive numerous signals of unlicensed activity in the financial sector, but usually try to address these through informal means (warning letters, information letters and information requests).[55] There have only been two formal interventions for illegal FIs (one for illegal banking activity and one of illegal payment activity), neither resulting in a fine. There are also a number of payment services that have registered as being exempted from licensing because the amount of payments they process are below the EU's Payment Services Directive threshold and are only domestic, but on investigation DNB has discovered that they are processing payments above the exemption threshold and to non-resident customers.

[55] DNB has received 41 signals of illegal payment service providers since 2016, of which 33 were issued warning letters.

389. There are currently 4.9 FTEs working on unlicensed activities across all sectors regulated by the AFM and 2.3 FTEs working on unlicensed activity across all sectors regulated by DNB. The Assessment Team does not consider this to be adequate to deal with the risk posed by the number of unlicensed and illegal operators operating across the financial sector and recommends that the resource levels, particularly in DNB, should be increased given it is now also responsible for dealing with unlicensed VASPs operating in the Netherlands.

BES Islands

390. Licensing and registration for FIs in the BES Islands is largely the same as in continental Netherlands. In addition, the propriety of policy makers is re-tested every three years, or before if there is a reason to suspect the person is no longer fit to hold their position.

VASPs

391. Since May 2020, DNB is responsible for the registration of some VASP activity defined by the FATF Standards. These services are custodian wallet providers and fiat to virtual asset exchanges (and vice versa), as required by the 5th European Anti-Money Laundering Directive.

392. The same market entry process for FIs applies to VASPs, including robust fit and proper assessments for all board members, day-to-day policymakers (including supervisory and executive board members) and controllers. There were 27 VASPs registered in the Netherlands at the end of the onsite and 216 fit and proper assessments had been carried out. No applications were rejected, but a number of applicants withdrew their applications, in one case where the applicant was being investigated as part of an ML investigation.

DNFBPs

393. There is one licenced casino in the Netherlands, and it is wholly owned by the Dutch Government. Ten policyholders were subject to fit and proper checks in 2019 and criminal records and certificate of good conduct as part of this process. Fitness and propriety of policy holders has only been a requirement since 2018 and the casino submits fit and proper reports on its policy holders annually. The Ksa is satisfied with the reports and there have not been any removals from positions based on this process.

394. There are also 10 licenced online gambling operators, which are licenced by Ksa and provide a range of gambling activities. Policy holders from online gambling are subject to fit and proper checks and must provide a certificate of good conduct. There are a number of illegal online gambling sites. Since April 2021, the Ksa has legal power to instruct banks and payment providers not to process transactions for these illegal sites and can impose a fine of EUR 820 000 or 10% of the bank's turnover in the preceding financial year if they ignore this instruction. No instructions had been issued at the time of the onsite. The Ksa has issued a number of fines to illegal online gambling sites, but often these fines are not realised because the operators are based outside the Netherlands. Because of an exemption by the Netherlands authorities, all other games of chance are exempt from AML/CFT licensing, registration and supervision.

395. Some DNFBPs in the Netherlands are licensed or registered by the relevant competent authorities and SRBs as outlined in Table 6.2. There are varying standards in the approaches taken to licensing across the various DNFBP sectors.

Table 6.2. DNFBP licensing/registration arrangements

Obliged entity	AML/CFT Supervisor	License/Registration
Casinos	Ksa	Licensed by Ksa
Real Estate Agents	BTWwft	-
DPMSs	BTWwft	-
Lawyers	Local Bar Presidents	Membership of the Netherlands Bar.
Civil Law Notaries	BFT	Appointed by the Ministry of Justice and Security and registered with KNB
Accountants (Auditors)	BFT	Register to NBA
Legal Advisors	BFT	-
Tax Advisors	BFT	-
Trust Offices	DNB	Licensed by DNB
Domicile Providers	BTWwft	-

396. Robust controls are in place for trust offices including the requirement to be licensed by DNB. These requirements were strengthened in recent years, due to the perceived high risk nature of the sector. Fit and proper checks are carried out on policy-makers, supervisory board members and BOs with shares of 10% or more in the organisation. The authorities could not provide figures on how many applications are rejected on fit and proper grounds, but indicate that rejection rarely occurs as applicants usually withdraw once there is an indication that their application may be rejected.

397. Illegal trust office activity is a significant issue and there are several initiatives underway to mitigate this risk, including the "FEC Project on Illegal Trust Service Providers" project as described below in Box 6.2. One of the main issues in the sector is trust offices avoiding stricter regulation by DNB by disaggregating their activity into services that are carried out separately and are therefore not licensed and subject to lighter touch supervision (e.g., domicile provision). Although it has been illegal to separate services in this way since 2019, it is difficult to detect. However, the authorities have had some success by working together to identify those involved in this activity. DNB and BTWwft, which supervises domicile providers, have begun collaborating by exchanging signals and information in order to try and identify illegal trust service providers. DNB participates in the FEC project and recently imposed a fine for illegal trust activity of EUR 361 500[56]. However, as mentioned above, the Assessment Team does not consider the resources for tackling illegal trust activity as sufficient.

[56] A fine of EUR 236 500 for the natural person involved, and a fine of EUR 125 000 for the legal person involved.

Box 6.2. FEC project on illegal trust activities

DNB, in collaboration with FEC partners FIOD, OM and Tax and Customs Administration, set up a targeted project to tackle illegal trust service providers. Trust offices that previously had licenses from DNB, but had given up their licenses, were the target of the project. DNB received signals that some of these offices were continuing to provide services despite no longer being licensed. This information was analysed and shared amongst partners. At the time of the onsite, cases were being researched in more detail and followed up by the FIOD.

398. Lawyers are registered by the NOvA, which maintains a register of all individuals admitted to the Netherlands Bar. Lawyers must provide the Bar with a certificate of good conduct, which is issued by the Ministry of Justice and Security and takes account of criminal records. NOvA believes that AML/CFT requirements only apply to a small number of lawyers, based on the self-declaration lawyers are required to submit annually indicating if they have carried out services within the scope of the Wwft.

399. Accountants are required to be registered or members of a professional body (NBA) and must provide certificates of good standing as part of the registration process. Notaries are appointed by the Ministry of Justice and Security. Appointment requires positive advice from the Admissions Committee for the Notarial Profession and from the Committee of Experts for the Notarial Profession and no objections against the appointment from the BFT and KNB. After receiving this information, the notary is appointed. Registration with the professional bodies mainly focusses on professional capability rather than fitness and propriety and registrants are not screened for criminal convictions. However, certificates of good conduct can also be requested as part of ongoing supervision. There are no licensing or registration obligations for other DNFBPs.

BES Islands

400. There are no entry controls for VASPs in the BES Islands and the authorities do not know of any operators located there. There are also no entry control requirements for most DNFBPs in the BES Islands. Trust offices are required to be licenced. The Joint Court of Justice of Aruba, Curaçao, Sint Maarten and of Bonaire, Saint Eustatius and Saba maintains a public register of all lawyers, who must provide a certificate of good conduct as part of the registration process.

Supervisors' understanding and identification of ML/TF risks

FIs

401. AFM and DNB have a good understanding of the inherent risks to the financial sector. This is informed through a range of information including NRAs, the SNRA, annual questionnaires, supervisory results and documents published by organisations, such as the Ministry of Justice and Security's National Coordinator for Counterterrorism and Security. The key threats identified by supervisors align with the NRAs and include TBML, underground banking and VAs. Lower risks include life insurance and pension funds. Both supervisors participated in the development of the NRAs through expert interviews and provided case studies and typologies from the financial sector.

402. AFM and DNB work with other authorities and engage with the private sector to inform their understanding of ML/TF risks and proactively disseminate to obliged entities information on what it identifies as the highest risks. Work on individual sectors is also carried out to enhance the understanding of the specific risks. For example, DNB collects quarterly transaction data from all money transfer offices. This information is used to construct risk profiles of transactions, customers, and networks to ensure the risk profile of the sector and individual institutions is up to date.

Box 6.3. Maintaining risk understanding and providing guidance

Several public incidents (FIFA corruption, Panama Papers, FinCen Leaks) prompted DNB to analyse the exposure of Netherlands' obliged entities to high profile financial crime issues. A questionnaire was circulated (in this case, to banks and trust offices), and the answers were assessed and risk determined on that basis. The risk in the trust office sector was determined to be high by DNB so it decided to investigate the sector and subsequently published questions and answers about the risks of providing TCSP services to customers with links to these high-profile international incidents.

403. DNB has a robust system in place for categorising individual firm risk. It recently moved to a new methodology Actualisatie Toezicht Methodologie (ATM), which aligns with the methodology used by the ECB for Single Supervisory Mechanism for banking supervision in the EU. The approach is largely driven by the obliged entities' responses to an annual questionnaire, which focusses on inherent risks and control measures. This is overlaid with additional information, such as outcomes from previous supervision, signals and incident reports and information from foreign supervisors. All firms are categorised by impact class, scores from the annual questionnaire and a range of supplementary information. AFM has a similar approach to categorising firm risk. It also uses an annual questionnaire, which focusses on inherent risk and control measures, as input for a quantitative model that generates AML/CFT risk scores. These risk scores, together with outcomes on previous supervision and professional judgement of supervisors most familiar with specific entities, serve to select entities for supervision. Like DNB's questionnaire, inherent risks include product risk, geographical risk and are tailored for each sector. Both supervisors use interactive dashboards to analyse the data.

VASPs

404. DNB carried out a comprehensive assessment of the VASP sector as part of its preparation for supervising VASP activity in the Netherlands. This involved consulting with the private sector, considering the NRA findings and engaging with other authorities, such as FIU-NL and LEAs. DNB uses the same ATM methodology to assign a risk rating to individual VASPs regulated in the Netherlands. The first annual questionnaire has been submitted by VASPs and DNB is using a dashboard to identify the highest risk firms for supervisory activity in 2022. Risks identified so far include a lack of compliance expertise within the VASP sector and the internal controls of VASPs not in line business expansion.

DNFBPs

405. There are varying levels of understanding of risk by DNFBP supervisors. The approach for trust office activity is the same as for other sectors supervised by DNB and is generally strong.

406. Understanding of the gambling sector is also reasonably strong, in part due to the small size of the sector and the fact that the Ksa has knowledge of all participants. The Ksa relies more on the SNRA for its risk understanding as casinos and games of chance are not covered in the NRA, despite casinos and other games of chance being cited as the highest risk in the Netherlands in a 2017 report.[57] The MoF and MoJ have undertaken two reviews of the games of chance sector (2017 and 2020). On the basis of these reviews, the ministries exempted all physical gambling except for casinos from AML/CFT supervision as they believe that these activities present low ML/TF risks.

407. For other DNFBP sectors, risk understanding is less developed. Sector risk assessments are largely based on the NRA and general risk guidance documents. This is supplemented by other information including signals of non-compliance in specific entities. Most DNFBP supervisors also participate periodically in a Wwft Supervision Meeting and other projects and fora where some aspects of risk are discussed (e.g., Consultation Team on Non-Reporting Entities, and the Obliged Entities Committee).

408. The NOvA circulated its first annual risk questionnaire in 2020 to its members in order to understand risks of non-compliance. The form includes questions on AML/CFT compliance, including whether the entity has performed activities that are in scope of the Wwft within the year. At the time of the onsite the responses to the questionnaires had not been used to inform the AML/CFT supervision strategy of local bar presidents, and the process of carrying out follow-up had not concluded.

57 Identifying and Assessing the Risk of Money Laundering in Europe research project, which was co-funded by EU Commission and involved the Netherlands MoF and MoJ.

409. The BFT has supervision arrangements with several professional bodies. Feedback from some of these bodies assists with its understanding of sector risk. For example, the accountancy professional body produces annual reports on the outcomes of the audits they carry out annually to accountants. In general, the majority of the audits result in a compliant or largely compliant result and it is unclear what emerging risk themes arise from this information. The BFT has identified inherent risks that apply across the sectors it supervises. The following are seen as higher risk entities: sole traders, newly established entities, unorganised entities (not members of professional bodies), entities with low UTR reporting behaviour and entities with customer portfolios with increased risk. It is unclear how the feedback or indicators informs BFT's supervisory strategy or leads to the targeting of resources to higher risk activity given that most of its supervision relates to investigating signals, including cases escalated as a result of peer reviews.

410. The BTWwft has five sector coordinators that have produced sector descriptions including on real estate agents, domicile providers and dealers in precious metals and stones. The sector descriptions contain examples of client, product, service, transaction/delivery channel and country/geographic risks applicable to the sector. The sector coordinators, gain knowledge from non-compliance of firms highlighted through triggers, FATF reports, information of the AMLC and engagement with the private sector. The sector descriptions are used as a guide for the supervisor to identify risks in individual firms, but are not used to determine a collective view of the risk across the sectors the BTWwft supervises, or to inform its supervision strategy and associated factors such as resource allocation.

411. Due to the size of the sectors and regulatory limitations (e.g., no registration requirements for most obliged entities) risk understanding for most DNFBPs is developed at sector and sub-sector levels. This is largely based on the NRA, signals from law enforcement and other authorities on potential non-compliance with obligations. At the time of the onsite, the Netherlands Tax Authority was working on a risk dashboard to assist BTWwft in developing its understanding of sectors, sub-sectors and obliged entities.

BES Islands

412. Supervisors in the BES Islands have a good understanding of risk. In 2019, AFM developed a Wwft BES risk model which allows them to conduct risk-based supervision and in 2020, developed a dashboard providing insights into individual firms and their inherent risks.

413. AFM and DNB annually request information from FIs and service providers in the BES Islands with respect to risks of ML, TF and compliance with sanctions regulations. On the basis of this risk questionnaire, AFM and DNB obtains insight into these various risks existing at the level of the individual institution. All FIs and service providers must complete the risk questionnaire.

Risk-based supervision of compliance with AML/CFT requirements

FIs

414. DNB and AFM apply a risk-based approach to supervision. Both authorities produce annual supervision plans. The plans prioritise the highest risk areas and enable them to effectively allocate supervisory resources. DNB moved to a new supervisory approach (ATM) in 2021, focussing more on risk analysis and available data. The new approach has two main categories: (i) scheduled supervisory activities (both a basic and a risk-based programme); and (ii) unscheduled supervision activities (supervision requests and unforeseen supervision activities, e.g., Panama Papers).

415. Scheduled supervision includes a basic and risk-based programme. The risk-based programme includes institution-specific (on-site and off-site) investigations for firms with higher risk profiles and (on-site and off-site) thematic work where information (e.g., data, intelligence or events) suggests there may be a sector-wide issue. Part of the risk-based programme also involves monitoring mitigation plans, where deficiencies have previously been identified. AFM also divides its approach between institute specific and thematic supervision and includes follow-up on remedial plans. DNB has approximately 60 staff across three financial crime supervision teams, which cover all sectors (228 entities). This has grown from approximately 30 since 2015, due to additional responsibilities and increased supervision. DNB believes further resources are needed in order to intensify integrity supervision and has requested this from the Minister of Finance. The AFM has 13 people responsible for AML supervision, this appears low given the number of organisations it supervises.

Box 6.4. Following up on remedial action plans

In 2017, DNB imposed an instruction and a fine on a bank for not reporting unusual transactions to the FIU-NL. In addition to the formal measures, the institution also had to draw up a recovery plan for the transaction monitoring and CDD process. DNB held 2-monthly meetings with the bank to monitor progress. In 2018, DNB carried out two validation studies. During the first validation study the deficiencies were found to be partially resolved, and in the second validation study the identified deficiencies had been fully resolved.

Institute specific investigations

416. DNB and AFM conduct off-site and on-site investigations. An off-site investigation can serve as a stand-alone investigation or can be the first phase of an on-site investigation. Since the start of the COVID-19 crisis in March 2020, all DNB on-site investigations have been conducted remotely. High risk banks are generally subject to a detailed assessment ("deep dive") every 3-5 years and medium risk banks 5-7 years. However, the three largest banks (covering 82% of the banking sector) have been subject to more intensive supervision in recent years as part of monitoring agreed remediation programmes. Up to five years for a detailed assessment into high-risk banks appears to be too infrequent and is possibly due to resource constraints. AFM has conducted 25 on site and 187 offsite investigations during 2020 and 2021.

417. Investigations generally focus on firms' risk assessments, policies and procedures, client files and completion of CDD, training manuals, transaction data, transaction monitoring and UTR reporting. Particular focus is placed on the design of a risk control framework and operational implementation. The supervisors choose the approach, including the specific on-site and off-site activities, most effective for the nature, scope and purpose of each investigation. The duration of visits by DNB varies from 3-4 weeks for standard investigations, but have taken up to three months in some cases. The inspection duration for AFM is much shorter. The number of onsite inspections for some sectors, such as life insurers and registered managers of investment institutions is low, which is in line with the risk profile of these sectors.

Table 6.3. Onsite inspections

Sector	2016	2017	2018	2019	2020	2021
DNB						
Banks	13	17	16	7	3	4
Insurers	3	7	3	2	1	-
Payment institutions	4	4	8	2	4	1
MTOs	3	3	5	5	3	3
Exchange institutions	-	-	-	3	1	-
EMIs	-	-	-	1	-	-
Safe custody service providers	-	-	-	4	-	-
AFM						-
Licensed (managers of) investment institutions	-	1	1	10	2	4
Registered (managers of) investment institutions	-	4	3	3	-	2
Investment firms	1	3	14	12	9	2
Life insurance intermediaries	2	-	5	-	7	
Total	26	39	55	49	30	16

*Covers the first half of 2021.

Table 6.4. Offsite inspections

Sector	2016	2017	2018	2019	2020	2021*
DNB						
Banks	36	7	88	2	13	14
Insurers	10	42	32	5	4	36
Payment institutions	20	1	32	2	4	10
MTOs	-	13	4	2	4	3
EMI's	-	-	-	-	1	2
AFM						
Licensed (managers of) investment institutions	1	11	2	9	15	22
Registered (managers of) investment institutions	-	-	-	-	18	59
Investment firms	-	3	22	9	26	36
Life insurance intermediaries	-	-	5	10	8	3
Total	67	77	185	39	93	185

*Covers the first half of 2021.

Thematic investigations

418. Thematic on-site investigations involving several institutions take DNB approximately one year to complete, with approximately six weeks available for each institution to be investigated. Thematic investigations can be the result of several risk drivers including incidents such as the Panama Papers, indications of risks in publications such as the SNRA, signals from other authorities or based on analysis of data from the annual questionnaires. For example, AFM conducted a thematic review in 2019 on transaction monitoring and mandatory reporting. This was in response to the 2018 risk questionnaire which showed that 27% of investment firms, 16% of (managers of) licensed investment institutions and 35% of registered (managers of) investment institutions had no automated or manual system to monitor customer transactions.

419. The number of onsite inspections has reduced significantly due to the COVID-19 crisis. This has led to more intensive offsite supervision and also meant more innovative use of data (e.g., the use of dashboards and outlier detections), particularly by DNB, in order to continue to maintain the intensity of supervision in higher risk entities.

Box 6.5. DNB anomaly detection model

Anomaly detection is a method to select potentially interesting customers (outliers) from a large dataset. The algorithm used is the isolation forest (a tree based model). This model works particularly well for large datasets. To give an approximation, the last time the model was used on a dataset consisting of over 300 million transactions and around 7.5 million clients.

The underlying thought is that some data points (clients) exhibit behaviours that the vast majority of clients do not. The outlier detection creates an overview with characteristics and scores of customers compared to other customers. The high scoring clients, the clients who have the largest change to be an outlier, are then selected for further in depth analysis by the supervisor instead of the manually selected files. The outlier detection model leads to more interesting files being identified and is a more risk-based way of doing research.

VASPs

420. DNB has three FTEs responsible for supervising VASPs. The same risk-based approach for FIs applies to VASP supervision. However, at the time of the onsite, the focus was mainly on the registration of firms and ensuring they understand their obligations. DNB is also harnessing blockchain analytics as part of its supervisory approach and has invested significantly in training employees involved in the supervision of VASPs. At the time of the onsite, one thematic investigation involving offsite inspections of 17 VASPs had taken place on the subject of reporting obligations, which resulted in a significant increase in UTRs across the sector.

DNFBPs

421. The Ksa conducts offsite and onsite supervision of the one casino (with several branches) since 2016. Supervision has focussed on understanding of obligations

following legislative change (AMLD4), CDD identification and verification, monitoring funds and source of wealth. Until January 2021, there was only one person responsible for AML/CFT supervision and enforcement. This number has now increased to three people due to the Ksa taking on responsibility for online gambling platforms.

422. DNB supervises licensed trust offices in a similar way to FIs, including the review of risk frameworks. Trust offices have a similar risk categorisation model as FIs and those with the highest risk receive the most supervisory focus. As mentioned previously, high risk activities include servicing conduit companies. There are between 30-40 high risk trust offices from a population of 154. Trust offices in the highest risk category are subject to continuous DNB integrity supervision. High risk trust offices are subjected to a deep dive investigation every two years. Investigations are often a combination of onsite and offsite supervision and can take up to 4-5 weeks with 3-4 days onsite.

Table 6.5. Trust office inspections

Activity	2016	2017	2018	2019	2020
Onsite (thematic and institute specific)	9	18	16	14	10
Offsite (thematic and institute specific)	40	-	8	13	21

423. DNB also conducts thematic reviews in the trust office sector and recently carried out an assessment of 21 trust offices that had not been inspected in the past three years[58]. DNB's thematic reviews can take up to eight weeks depending on the scope and number of firms included.

Box 6.6. Thematic investigation in the trust offices sector

DNB defines a "whitespot" as a trust office that has not been supervised by DNB for at least three years. As there is a relatively large number of whitespots, DNB opted for an investigation where a large number of trust offices can be assessed.

In order to find out as efficiently as possible what the level of compliance is, and thus the potential integrity risk, an offsite was conducted into the integrity policies at trust offices that qualify as whitespots. Over a period of four months, DNB investigated 21 trust offices, allowing it to risk score these institutions for more focused supervision. The desk-based exercise found that of the 21 institutions, nine (43%) scored "poor" and two (10%) scored "good" in terms of the policies they had in place. Overall, 52% presented a risk with regard to the set-up of the integrity policies. The investigation resulted in the revocation of the licence of one trust office. The nine trust offices which scored "poor" are the subject of a follow-up investigation.

58 The assessments of 21 trust offices as part of the thematic review are also reflected in table 6.5

424. Other DNFBP supervisors do not classify their entities/professions based on risk, instead their investigations are mostly based on reactive signals from outside sources (e.g., LEAs) and lack of resources drives this supervisory approach.

425. The NOvA has 11 local Bar presidents responsible for supervision. Approximately 10% of law firms in their region are inspected annually, but not all are inspected for AML/CFT purposes. Onsite inspections take approximately two hours each. The NOvA carried out a thematic review of 50 firms in 2019/2020 and covered a number of areas (e.g., CDD, UTRs). The firms were selected on the based on whether they indicated they carried out activity covered by the Wwft. The NOvA found that the majority of firms reviewed as part of the thematic work executed proper CDD and carefully considered whether UTRs should be reported to FIU-NL.

426. The BFT estimates it is responsible for the supervision of approximately 49 000 (junior) notaries, independent legal advisers, accountants, and other entities, such as tax advisors. BFT has supervisory arrangements with the Association of Registered Accountants (SRA) to coordinate peer reviews in their sector and there is a legal requirement for notaries to be peer reviewed by the KNB every three years on the implementation of legal requirements and office procedures, including AML/CFT compliance. Element of the peer review rated insufficient can be remediated by the obliged entities by an improvement plan, which is followed up. More serious failings from the peer review audits can be escalated to the BFT for formal or disciplinary action. A large majority of audits are compliant or largely compliant. Again, this appears to be out of line with the risk profile and understanding of AML/CFT obligations in the sector. The BFT has approximately 15 FTEs and carries out reactive investigations based on signals from other authorities (e.g., FIU-NL). There have been between 20 and 45 of these each year since 2016.

427. The BTWwft supervises over 100 000 entities, including those that carry out activities in higher risk sectors (e.g., real estate), and activities that are not covered by the FATF Standards (e.g., vehicle traders sector). There are 30 FTEs that cover AML/CFT supervision across all sectors. The BTWwft has a three pillared approach: signal-based inspections, thematic inspections, and risk-based selections of firms identified in the supervised sectors. The thematic inspections and risk-based selections are currently determined by the sector coordinators' understanding and judgement. The introduction of a risk dashboard, which was being developed at the time of the onsite, should enhance the BTWwft's ability to select areas and entities of focus in a more advanced way. Since 2016, BTWwft has carried out thematic work in the real estate sector (mainly in holiday homes), but there have been no thematic reviews specifically aimed at other sectors within scope of the FATF Standards. The BTWwft carries out approximately 1 100 investigations a year, around half of which are onsite. Approximately half of these are focussed on entities that fall outside the scope of the FATF Standards.

428. There is currently no explicit obligation for DNFBPs other than trust offices to screen their clients and transactions against PF and TF sanction lists. Since there is no obligation, supervisors have no remit to supervise compliance, nor can they apply sanctions or remedial actions for non-compliance. As noted under IO.11, in relation to PF TFS, many DNFBPs interviewed during the onsite visit indicated that they do screen their clients against sanctions lists. The Assessment Team considers that the lack of an explicit obligation to perform sanctions screenings and a supervisory framework to monitor compliance may impact the timely implementation of TFS.

BES Islands

429. Approximately three AML/CFT supervisors from DNB (two FTEs in total) visit the BES Islands three times a year for one week of supervision. These visits are aimed primarily at Bonaire. The last visit to Saba and St Eustatius was in 2017, as supervision in these islands takes place on a five-year cycle.

430. The BTWwft supervises all DNFBPs in the BES Islands, except for casinos and trust offices. Generally, the BTWwft visits the BES Islands annually for 2-3 weeks and carries out onsite investigations. These investigations are conducted by four inspection officers in pairs. At the time of the onsite, the BTWwft had not reviewed the files of the two notaries in the BES Islands who act as gatekeepers for real estate and company formation. Before 1 July 2021, the BTWwft did not have powers enabling it to carry out these types of reviews. Now that the powers are in place, the Assessment Team believe this should be a priority given the risks associated with notaries and their main activities. DNB conducted onsite inspections in 2017 to the two casinos and one trust office in the BES Islands.

431. The same absence of a requirement for DNFBPs except trust offices in the Netherlands for TFS screening, exists for all DNFBPs and VASPs in the BES Islands.

Remedial actions and effective, proportionate, and dissuasive sanctions

FIs

432. DNB and AFM widely employ remedial actions where they identify failures in compliance in line with their joint enforcement policy. Reports with remedial actions are issued to obliged entities after most DNB investigations. The supervisors place significant emphasis on following up on remedial action plans and in significant cases generally require FIs to report on progress on a quarterly basis. Remediation is also followed up in subsequent investigations. Several large banks currently have extensive longer term remediation plans in place, which are often based on measures imposed by DNB. In some cases the banks have engaged third parties to assist them in monitoring progress against these plans. In recent years, the authorities have placed significant emphasis on improving firm culture as a way of setting the right tone from the top and stressing the importance of compliance. Often remediation plans include root cause analysis of failures resulting from poor compliance culture. Remedial actions are used alongside, and as part of, formal and informal enforcement action.

433. DNB and AFM, have a joint enforcement policy and can impose several types of formal and informal measures depending on a number of factors, including severity of violations, culpability and compliance orientation of the FI in scope, supervisory history of the FI (i.e., outcome of previous investigations and/or measures imposed in the past), similar cases, and if remediation is already underway. Informal measures include a compliance briefing or a warning letter. Formal actions include: an instruction; order subject to a penalty; administrative fine; disqualifying policymakers from exercising their profession; and a public warning. An administrative fine has a punitive character. All other formal and informal measures are remedial in nature.

434. When DNB finds AML/CFT failings, it develops an intervention strategy taking into account the enforcement policy factors mentioned above. Most intervention strategies include a proposal to impose sanctions or other enforcement measures. Before formal enforcement measures are imposed, the FI is notified. At this point, the FI often begins remediation or may have already begun doing so. Supervisors are required to include the scope of remedial actions being undertaken by the FI as part of the decision making on whether or not to impose an enforcement measure. If an FI demonstrates that it is willing and able to remediate the violations within a reasonable timeframe, DNB often does not apply immediate enforcement measures. In cases where an informal measure is being imposed (i.e., no formal enforcement measure is imposed), the failing is not made public and the name of the firm is not published, except in exceptional cases. Formal measures are largely preceded by informal measures. This can create a delay in resolving issues and preventing the continuation of violations. The authorities also described how in some cases it had taken over one year to follow-up on unanswered warning letters. DNB can apply formal and informal measures and has done so in some cases.

Table 6.6. Number of formal and informal measures applied by DNB (excluding trust offices) and AFM

	2016		2017		2018		2019		2020		2021*	
Informal	DNB	AFM	DNB	AFM	DNB	AFM	DNB	AFM	DNB	AFM	DNB (Q1 and Q2)	AFM (Q1 – Q3)
Compliance briefings	2	1	3	1	5	0	6	0	3	1	1	2
Instruction letters on compliance with standard	0	0	0	9	0	1	0	5	0	4	0	5
Warning letter	0	0	0	0	2	3	4	64	3	31	4	32
Conversation on compliance with standard	0	0	0	0	0	0	0	0	0	12	0	6
Information letter on compliance with standard	0	0	0	0	0	0	0	73	0	141	0	108
Formal[59]												
Instruction or intended instruction	4	0	3	1	1	1	7	1	0	3	1	4
Order subject to a penalty, or intended order subject to a penalty	2	0	0	1	1	2	0	1	2	3	0	6
Administrative fine, or intended administrative fine	4	0	2	0	1	0	7	0	9	0	1	3
Revocation of license, or intended revocation of license	0	0	0	0	0	0	1	2	0	0	0	0
Report to public prosecutor	0	0	0	0	0	0	0	0	0	0	0	0

*DNB data covers the period up to June 2021.

59 DNB figures are imposed formal measures. AFM figures include intended formal measures.

6

435. The Wwft was amended in July 2018 allowing DNB and AFM to impose higher fines than previously available, including up to 20% of a firm's annual turnover if the amount is higher than twice the upper limit of the third fine category (i.e., more than EUR 10 million). The below table outlines the current fine categories. In practice, the largest fine imposed to date is less than 5% of a firm's annual turnover.

Table 6.7. Fine categories as of July 2018

Fine category	Basic	Minimum	Maximum
1	EUR 10 000	EUR 0	EUR 10 000
2	EUR 500 000	EUR 0	EUR 1 000 000
3	EUR 2 000 000 / 2500 000	EUR 0	EUR 4 000 000 / 5 000 000

436. Recent legislative changes also permit the publication of all formal measures. These developments have had a positive effect in terms of dissuasiveness, but the number of formal measures imposed remains low, particularly by AFM. DNB and AFM do not have powers to take criminal enforcement action for AML/CFT failings. However, in the case of serious violations, DNB and the AFM refer cases to a Steering Team on Supervision (which includes DNB, AFM, FIOD and the OM). The Steering Group then decides on the most appropriate action for the particular case (administrative fine or prosecution). Under Dutch law, an administrative and a criminal sanction cannot be imposed in the same case. The Steering Group has considered 68 DNB cases since 2016, dealt with 53 cases under administrative law, and 15 cases under criminal law (this includes trust offices and VASPs). Five AFM cases have been considered since 2019 and all of these have been dealt with under administrative law.

437. Two recent high profile settlement cases against two of the largest FIs in the Netherlands have had a significant impact on the prioritisation of AML/CFT compliance across the banking sector. This has also had a cascading effect on other sectors and was frequently mentioned by private sector representatives met by the Assessment Team. Although the amounts of the settlements are large (EUR 775 million and EUR 480 million, respectively), they relate to AML/CFT failings that occurred over a number of years, with the banks receiving repeated warnings and enforcement measures from DNB, which did not have the required impact. The below case study highlights one of these cases.

Box 6.7. Settlement involving major bank

In September 2018, a large bank entered into a settlement agreement with the Dutch Public Prosecution Service following a criminal investigation which revealed that criminals had laundered money through its accounts due to serious shortcomings in its AML/CFT framework and culpable money laundering. The shortcomings identified resulted in clients being able to use their bank accounts for ML practices over several years.

Dutch financial crime prosecutors stated that the bank had violated AML/CFT laws "structurally and for years" by not properly vetting the BO of client accounts and by not identifying associated unusual transactions.

The OM started its investigation in 2016 after identifying a pattern of violations. They cited four case examples where the bank's accounts were used for criminal activities, most notably for bribes paid by a telecommunications company in Uzbekistan.

The bank agreed to pay EUR 775 million to settle the case.

VASPs

438. The same DNB process for remedial and punitive measures applies for VASPs. Due to the early nature of the regime, no remedial actions have been imposed to date. DNB has issued informal warning letters to businesses operating as VASPs that had not applied for registration. DNB has also issued a public warning in relating to one illegal VASP and is considering enforcement action in other cases.

DNFBPs

439. Apart from the trust office sector, there is significant variation in terms of the application of remedial actions applied by supervisors in other sectors. Informal measures are applied in many cases and mainly to apply for failures in reporting UTRs. The application of remedial actions are not always applied consistently by different supervisors.

440. DNB applies the same approach to remedial and punitive measures for trust offices as for FIs. A number of informal and formal actions have been imposed on trust offices in recent years following thematic reviews.

6

Table 6.8. Formal and informal measures applied by DNB to trust offices

	2016	2017	2018	2019	2020	2021*
Informal						
Compliance briefings	0	1	1	0	1	0
Instruction letters on compliance with standard	0	0	0	0	0	0
Warning letter	0	0	2	0	3	0
Conversation on compliance with standard	0	0	0	0	0	0
Information letter on compliance with standard	0	0	0	0	0	0
Formal*						
Instruction or intended instruction	14	9	5	6	6	2
Order subject to a penalty, or intended order subject to a penalty	5	5	3	6	5	0
Administrative fine, or intended administrative fine	3	3	2	4	7	4
Revocation of license, or intended revocation of license	3	3	3	1	0	0
Report to public prosecutor	1	2	0	0	0	0

*DNB data covers the period up to June 2021.

441. The Ksa has imposed fines on illegal land based and gambling providers. The amounts of fines imposed for illegal online gambling sites appear appropriate, but less than half of these have been recovered in practice.

442. The BFT can fine a percentage of a firm's turnover for AML/CFT failings. Fines range from 1% to 5% depending on the gravity, duration and culpability. In cases where 4 or 5% is considered, the supervisors liaise with the OM to determine whether a criminal prosecution should take place instead. The NOvA states that local bar presidents prefer to use disciplinary law rather than administrative law when AML/CFT failings are identified. NOvA also states that lawyers see disciplinary measures as more serious than other measures such as administrative law sanctions because of the reputational damage they cause. Disciplinary measures include a reprimand, suspension and disbarment, as opposed to administrative law, which includes an administrative fine and order subject to penalty. Both disciplinary and administrative measures can be published. Approximately 7% of complaints registered with the NOvA led to disciplinary measures. Since 2016, there have been 24 disbarments, 45 suspensions, and 19 administrative measures which include AML/CFT failings. The case below demonstrates the use of disciplinary measures to address failings including poor CDD measures. Although disciplinary action by the Bar presidents can have a significant impact on lawyers, they are infrequent and not always proportionate or dissuasive.

Box 6.8. Disciplinary case for a lawyer

On 23 December 2019, the Hague Board of Discipline suspended a lawyer for 26 weeks with an additional eight weeks suspended for two years subject to no further breaches.

The violations of the lawyer included failure to conduct CDD, providing money management services, taking funds into custody without a reasonable purpose, misuse of a client trust account, making improper cash payments to his client and failure to report UTRs.

The lawyer's client was declared bankrupt in 2011. Shortly after, the individual was given EUR 50 000 as a deposit for a new project. Instead of receiving the money in his own account, the client asked the lawyer to receive the payment in order to disguise it and ensure the funds were not subject to bankruptcy measures. The lawyer agreed and accepted the funds into the trust account of his own office.

In the period between 2013 and 2016, the lawyer used funds to pay mortgage debts for his client amounting to EUR 30 000, made a EUR 5 000 cash payment to his client and paid 15 000 into an account for his client and disguised this as a loan.

443. Other formal measures available to DNFBP supervisors are the ability to impose performance improvement plans and cease and desist orders. Performance improvement plans involve a letter to the reporting entity with an instruction that has to be followed within a certain timeframe or that the entity has to improve internal procedures. In case a reporting entity fails to comply, a cease and desist order can be imposed.

444. When a cease and desist order is not followed by the obliged entity within the given time limit, this can result in a financial penalty. In practice, informal warning notices and other informal measures are heavily relied on by some supervisors and formal measures are only applied to a limited extent. The BFT imposes more formal measures than informal measures. These are mainly performance improvement plans and can be a result of an issue being escalated by one of the professional bodies it has agreements with.

Table 6.9. Fines imposed on DNFBPs

		2016	2017	2018	2019	2020
Illegal Land based betting	Number	1	0	2	1	1
	Amount	373 750	0	37 300	11 056	86 528
Illegal online betting[60]	Number	0	7	5	11	2
	Amount	0	907 000	1 322 000	3 480 000	600 000
Real Estate Agents	Number	21	22	18	10	1

60 Fines imposed include to non-Dutch entities. Approximately half of the fines imposed have been recovered.

		2016	2017	2018	2019	2020
	Amount	26 250	29 400	32 100	12.200	20.000
DPMS	Number	0	1	2	1	4
	Amount	0	10 000	7500	1000	100 000
Lawyers	Number	0	0	0	0	0
	Amount	0	0	0	0	0
Notaries	Number	1	1	2	1	3
	Amount	10 000	6 000	51 000	8 500	129 300
Accountants	Number	23	6	16	20	0
	Amount	175 140	126 222	146 133	212 995	0

BES Islands

445. Most AML/CFT failings in the BES Islands are addressed through informal measures and any fines that have been imposed are very low.

Impact of supervisory actions on compliance

FIs

446. The authorities believe that FI compliance culture, particularly in banks, has shifted as a result of guidance and other measures and the aforementioned high profile settlement cases against two of the largest Dutch banks. Awareness of the role of AML/CFT gatekeeper was relatively low until 2015, but in recent years has improved considerably. Obliged entities are now aware of their responsibilities and there are recognised improvements. DNB and AFM monitor and validate remediation plans that have been put in place. Although this can be seen as resource intensive, it provides confidence to the authorities that the plans are properly executed and the intervention has delivered results.

447. There has been a significant increase in the number of UTRs submitted to FIU-NL between 2017 and 2020 (see IO.4). Furthermore, there was a gradual increase in the number of TFS reports between 2015 and 2020. DNB attributes this to the wide-ranging thematic reviews that took place from 2016 onwards, as well as the large settlement cases. For example, following the major settlements, the supervisors observed many institutions carrying out bank-wide CDD remediation projects, investing in new technology for CDD and transaction monitoring and significantly expanding their first and second-line defence functions.

DNFBPs

448. Since 2016, DNB has seen a number of licensed trust offices cease trading (238 in 2016 to 162 in 2020). Although there are several factors that may have contributed to this reduction, DNB attributes some to the outcome of stricter regulations and more intense supervision of obligations. DNB sees improvements in the sector, but still finds that CDD is often not carried out sufficiently.

449. In general, DNFBPs supervisors are not able to provide figures on the impact of their supervisory interventions, but often an increase or decrease in UTRs is referred to as a proxy. The BTWwft reports that in 2018 more than 60% of the re-inspections carried out, the obliged entity had rectified identified issues. In just under 40% of the cases, violations were repeated. In more than 10% of the cases, the violations were so serious that the case was referred to a penalty payment officer for a fine to be considered.

BES Islands

450. Supervisors often see a direct impact of their supervision through monitoring, due to the small number of entities on the islands. Formal measures such as instructions were not able to be published before July 2021, undermining the deterrent effect of formal interventions.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

FIs

451. DNB and AFM undertake a range of outreach activities. This includes publishing newsletters, organising seminars, issuing AML/CFT policy documents, and publishing Q&A's on a range of issues such as transaction monitoring and integrity risk of football. Both supervisors communicate to a wide population through monthly digital newsletters that set out legislative changes, risks that have been observed in various sectors and best practices. The newsletters are also used to provide generic feedback on investigations.

452. DNB and AFM publish a supervision agenda on an annual basis listing the primary financial market risks and the main supervision focus. DNB and the AFM are active members of the FEC. This is a partnership of public and private parties cooperating in various projects, including the FEC-OM real estate project. More recently, a TF and Serious Crime Task Force was established to cooperate with banks to exchange information and establish typologies, allowing FIs to more easily identify unusual transactions. DNB acts as an observer in these task forces. Both supervisors work closely with the various sector professional bodies, who disseminate information to their members.

453. Both supervisors provide guidance for all sectors they supervise. However, FIs met during the onsite commented that guidance could be more specific and provide more detailed examples of good practices in complying with AML/CFT obligations.

VASPs

454. DNB has undertaken significant outreach with the VASP sector to enhance its understanding of the Dutch VASP population and ensure VASPs understand their AML/CFT risks and obligations. This outreach began in advance of DNB taking on supervisory responsibility for VASPs. DNB has also held outreach sessions with obliged entities, produced guidance on its website and has sent five newsletters to over 13 00 subscribers.

DNFBPs

455. DNFBP supervisors invest a significant amount of resources in engaging with sectors to ensure they understand their AML/CFT risks and obligations, such as through presentations, guidelines, Q&A documents and good practice documents.

456. Extensive guidance has been produced for all DNFBP sectors. However, some entities met during the onsite noted that the guidance could be more detailed, particularly for smaller entities. BTWwft provides risk matrices for each supervising sector to promote a clear understanding of risks. The matrices provide generic risk indicators for client identity, service, transaction and country risk.

457. DNB, BFT, BTWwft and NOvA all have help desks enabling entities to ask questions via website, email or telephone. Many obliged entities met during the onsite appreciated the ability to easily contact the supervisors with questions.

BES Islands

458. Many of the communications produced for obliged entities in the Netherlands also apply to the BES Islands. Specific outreach activities are also conducted, including seminars, preparation of guidelines, and frequently asked questions. DNB has developed a website specifically for the Caribbean Netherlands. In 2021, DNB published the Good Practices Wwft BES, a guidance specifically aimed at the institutions on the BES and the local risks and regulations.

Overall conclusion on IO.3

1. DNB and AFM supervise FIs, VASPs and trust offices and have robust entry controls in place to ensure controllers and senior managers are fit and proper. However, despite having a significant number of illegal operators, including underground banking and illegal trust offices, there is a lack of resources to address the problem.
2. Understanding of risk by DNFBP supervisors is generally less granular than that of DNB and AFM. Although certain aspects of risk based supervision have been introduced by some DNFBP supervisors, major improvements are needed to ensure effective risk-based supervision is applied across all DNFBP sectors.
3. The recent high profile settlement cases against two of the largest FIs in the Netherlands have had a significant impact on the prioritisation of AML/CFT compliance across FIs and more broadly. While this is a noteworthy development, the duration of these AML/CFT failings over several years is indicative of a lack of dissuasiveness of earlier interventions.
4. Some supervisors rely heavily on warning letters and other informal sanctions, even for more serious breaches of regulation, including unlicensed activity. This does not always have a deterrent effect and means that issues may go unaddressed longer than they would if formal measures were applied.
5. The Netherlands is rated as having a moderate level of effectiveness for IO.3.

Chapter 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

1. The Netherlands CoC commercial register contains comprehensive basic information on all legal persons established in the Netherlands. Since September 2020, all newly created legal persons must also register BO information on the CoC's BO Register. Existing legal persons have until 27 March 2022, to register BO information. At the time of the onsite, only 27% of existing legal persons had registered BO information in the BO register.
2. A notarial deed is required for the establishment of most legal persons in the Netherlands and there are clear requirements for legal persons to provide accurate and up-to-date information and to notify the register of changes. All registrations are checked by CoC for completeness and consistency with the Personal Records Database, company register and documents provided. When inaccurate information is submitted by notaries, this is not followed up with the notary who submitted it.
3. As noted under IO.1, authorities have launched initiatives aimed at identifying and assessing ML/TF risks of legal persons. These include thematic projects conducted by FIU-NL (e.g., on NPOs), AMLC (Offshore and No Shelter), and FEC (rogue foundations). However, these initiatives do not provide a clear and comprehensive overview of the risks posed by legal persons. The result is that authorities and obliged entities have an inconsistent understanding of the main ML/TF risks related to the different types and sub-types of legal persons in the Netherlands.
4. Legal arrangements, such as trusts, cannot be set up under Dutch law (with the exception of mutual funds). The Netherlands recognises foreign trusts established under the law of other jurisdictions and estimates there are approximately 15 000 legal arrangements operating in the Netherlands.
5. The Netherlands relies on FIs and DNFBPs as gatekeepers to prevent the misuse of legal persons and arrangements and to improve the quality of the data in the BO register by reporting discrepancies. Given that many recent fines and other sanctions imposed on obliged entities (including high profile fines against the largest FIs) relate to CDD failings, including failure to properly identify BOs, it is not clear how effective this measure is ensuring the accuracy of information in the register.
6. Aside from dissolving legal entities, no sanctions are imposed for failing to provide correct or up-to-date basic information. Sanctions for failure to submit financial statements have been imposed, but these are not dissuasive given the remaining

7

high levels of noncompliance. No cases of providing incorrect BO information that is punishable have been detected so far.

7. The Netherlands allows, under strict circumstances, obliged entities to accept senior managing officials as so called 'pseudo BOs'. Although this option is only meant as a last resort, obliged entities will often make use of it as soon as it is clear that there is no natural person with more than 25% of the shares, voting rights or ownership interest in that entity, without further verifying if there are no natural persons owning or controlling the legal person by other means. This is likely to occur more often in high risk, complex international constructions, such as conduit companies. This practice has led to cases where notaries identify trust office employees who act as nominee directors as the pseudo BOs (and apply EDD measures such as an examination into their source of wealth on them), while the ultimate BOs may remain unknown.
8. There are several deficiencies in the BES Islands, including a lack of a requirement for legal persons or arrangements to hold BO information.

Recommended Actions

1. As noted in IO.1, the Netherlands should undertake analysis and produce a clear and comprehensive overview of the risks posed by legal persons. This should include a refined assessment of the risks of foundations, making a distinction between the different purposes for which this legal form is used (charitable, non-charitable, STAK, etc.) and the potential ML/TF risks of the legal form of church communities. The authorities should follow-up on the findings of the reports on illegal trust offices and on conduit companies.
2. Authorities should consider proportionate enforcement action against notaries who fail to submit accurate basic and BO information to the CoC registers. The Netherlands should continue its efforts to ensure the BO register is populated with accurate information on the BOs of legal persons active in the Netherlands, including giving targeted guidance in order to limit the registration of senior directors as 'pseudo' BOs to an absolute minimum.
3. The Netherlands should continue efforts to complete the legislative process and start registering the BOs of trusts and similar legal constructions.
4. The NL should take measures to reduce the risk of ML abuse by conduit companies.[61] These measures should include gaining a better understanding of the

[61] The term "conduit company" refers not to the strict legal definition of the Wtt 2018, but to companies with features that are typical for a conduit company. Typically, a conduit company would be a Dutch legal entity, with little or no real presence in the Netherlands, that is part of an international structure and that has been set up for tax, financial or legal purposes. Conduit companies often have substantial balance sheet positions and/or have significant amounts of money flowing through them coming from or going to foreign entities that are part of the same structure.

ML/TF risks of conduit companies, strengthening financial reporting obligations and reviewing the possibility to register senior managing directors of a conduit company ('pseudo' BOs) and strengthening safeguards if found that this is misused for concealment of the ultimate BOs.

5. The Netherlands should ensure that sanctions are proportionate and dissuasive for failure to submit and maintain accurate information on CoC registers, particularly in cases involving intent.

6. The Netherlands should require legal persons in the BES islands to hold BO information and ensure this is available to competent authorities in a timely manner and should ensure legal persons are complying with their CoC register obligations.

459. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40.[62]

460. The Assessment Team's findings on IO.5 are based on discussions with Netherlands authorities and obliged entities, and information provided by the authorities including the NRA and case studies.

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

461. Information on the creation and types of legal persons is publicly available through the CoC website and several other sources. The CoC website provides user-friendly instructions on the requirements to establish and register a Dutch legal person and register a foreign legal person that seeks to establish a branch office or commercial undertaking in the Netherlands (in both Dutch and English). This site includes step-by-step guides and forms (primarily to be filed by civil law notaries).

462. Most legal persons must register their basic and BO information in the CoC company register (Handelsregister) and BO register respectively. This includes foreign legal persons that have a branch office or commercial undertaking in the Netherlands, of which there are 8 000 registered with the CoC in the company register.

[62] The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

463. The requirement to register BO information is relatively recent as it came into force in September 2020. At the end of the onsite, the BO register contained BO information on approximately 27% of all existing legal persons. Existing legal persons (created before September 2020) have until end March 2022 to register BO information at the CoC. Newly created legal persons (established after September 2022) must provide this information upon establishment at the CoC. All changes to basic and BO information must be entered on the register within one week of the change. Obliged entities, which have the obligation to check the information in the BO register when performing CDD, that find discrepancies between information in the BO register and other information collected in the course of CDD are required to report the discrepancies to the CoC. Based on interviews with obliged entities, they are submitting these discrepancy reports regularly.

464. Private limited companies are the most common type of legal person and make up approximately 60% of all legal persons (see table 1.2 in Chapter 1 for a complete overview of legal persons in the Netherlands). Legal arrangements such as trusts cannot be created in the Netherlands with the exception of mutual funds, but foreign trusts and legal arrangements can and do operate within the jurisdiction. Foreign legal arrangements in the Netherlands are subject to strict tax legislation and the Tax and Customs Administration collects relevant information. The Dutch authorities have estimated that there are approximately 15 000 legal arrangements, including mutual funds, in operation in the Netherlands.

BES Islands

465. Legal persons in the BES Islands are created in the same way as the continental Netherlands and basic information must be registered in the company register. There is no requirement for legal entities to hold BO information or to register BO information in a central BO register. As in the continental Netherlands, obliged entities in the BES Islands need to register, identify and take reasonable measures to verify the identity of BOs as part of CDD obligations.

466. Bonaire has its own company register and there is a joint register for Saba and St. Eustatius. The company registers are publicly available, but at the time of the onsite were unavailable online due to a technical issue. LEAs require a subpoena to access non-public information, shareholders decisions or other information deposited at the company registry. Although the authorities suggest this is a straightforward process, and this information is available on a timely basis when needed, it does increase the time required to obtain the information. Express trusts cannot be established in the BES Islands, although foreign trusts are recognised and do exist in the jurisdiction. Mutual funds can be created in the BES Islands, but according to the tax authority there are currently no open mutual funds in operation. Open mutual funds are required to register with the AFM. Bonaire has 42 private foundations, a specific type of legal person that does not exist in the Netherlands, which has features that pose specific risks for ML/TF, including:

- no prohibition to distribute profits for private purposes (unlike 'ordinary' foundations);
- possibility to create a legally non-binding set of written wishes or a (to a certain degree) legally binding document with 'instructional authority' for the board by means of a private deed, e.g., the BO itself can be appointed; and

- ability to receive or make tax-free donations/distributions not taxable with in the Caribbean Netherlands with withholding tax or income tax, provided that effective management of the private foundation is located outside of the Caribbean Netherlands and the receiver is not a resident of the Caribbean Netherlands.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

467. As noted in IO.1, the Netherlands does not have a comprehensive assessment of the ML/TF risks associated with the different types of legal persons including vulnerabilities due to their features and the way they are used. As a result, the ML NRA does not identify any heightened ML risks with particular types of legal entities, although certain unusual situations (e.g., directorship in more than 50 legal entities or board changes in a short period of time) are mentioned. The TF NRA notes that foundations in general are more vulnerable than other entities to TF abuse, but does not differentiate between the different uses of foundations (e.g., charitable and non-charitable).

468. The Dutch authorities have undertaken various initiatives that focus on specific legal persons and arrangements and their associated ML/TF risks. The initiatives include AMLC analysis on the frequency that certain types of legal persons appear in criminal investigations, a public-private partnership project by the FEC on rogue foundations, FIU-NL typology work on NPOs and a report commissioned by the Ministry of Finance on illegal trust services. Offshore companies involved in the purchase of real estate are identified as high risk and the AMLC "Offshore Project" was established to gain further insight into this area. In addition, the AMLC "No Shelter" project was established to better detect the existence of (legal or illegal) service providers engaged in ML/TF through concealing (international) company structures. The use of domicile addresses has been identified as a higher risk for BO concealment. The Dutch authorities and some obliged entities also identify foundations, limited partnerships and church communities as presenting a higher risk for ML and TF, but certain measures such as voluntarily seeking an ANBI-status and/or CBF-seal for charitable foundations are partial risk mitigation measures (see IO.10 for more information on the charitable ANBI status and CBF seal for fundraising). In addition, the use of complex structures involving any type of legal entity and the amount of conduit companies active in the Netherlands pose ML/TF risks.

469. Legal arrangements such as trusts cannot be established in the Netherlands, with the exception of mutual funds. There are currently around 2 800 open mutual funds registered with the AFM, and up to 15 000 legal arrangements in operation in the Netherlands. The Netherlands recognises foreign trusts and maintains information on foreign trusts holding real estate in the Netherlands. The Dutch authorities also have an understanding of the investments of legal arrangements operating the Netherlands through DNB's supervision of trust offices. In addition, obliged entities have to register, identify and take reasonable measures to verify the identity of BOs of legal arrangements, including foreign legal arrangements as part of their CDD obligations. The Wtt 2018 requires that trust offices identify the BO of the trust and conduct a risk analysis and CDD on trusts that they manage.

BES Islands

470. Competent authorities understand the risk of legal persons in the BES Islands and have identified abuse of legal entities purchasing real estate as the key risk in the NRA.

Mitigating measures to prevent the misuse of legal persons and arrangements

471. The Netherlands places significant emphasis on notaries as gatekeepers for preventing the misuse of legal persons. Most legal persons must be created with the use of a civil-law notary. However, notaries have a legal 'ministerial duty (ministerieplicht)' to offer the full range of notarial services to the public and must accept all customers, unless there is a sound reason not to do so. In practice, notaries almost never refuse services to clients, including for drafting deeds for the establishment of a company. A notarial deed is not required for the establishment of church communities or partnerships (or other legal entities) without legal personality, such as limited partnerships. During the onsite visit, the Assessment Team heard of instances in the misuse of certain types of legal persons in order to avoid the notarial gate-keeper. For example, some obliged entities met during the onsite gave anecdotal accounts of massage parlours and other cash intensive businesses being set up as church communities. As a result, the assessment team is concerned that the ministerial duty of notaries to provide services conflicts with their role as gatekeeper to refuse or exit customers on CDD grounds. Moreover, the possible remaining vulnerabilities due to less mitigation measures for church communities and some other legal entities could negatively impact the Netherlands' effectiveness.

472. The Netherlands introduced the Judicial Agency for Testing, Integrity and Screening (JustisTRACK) automated information system in 2011. This information hub is managed by the Ministry of Justice and Security and continuously monitors the integrity of legal persons, including the directors and affiliated persons or legal persons. The system uses several data sources to automatically screen persons registered in the CoC and issues risk reports to LEAs and investigative/supervisory bodies who can initiate investigations when enhanced risk situations are identified (e.g., directors with criminal history are listed as company directors). Not all supervisory bodies have access to the reports. This is a weakness and should be addressed in order to strengthen the capabilities of the smaller regulators.

Box 7.1. JustisTRACK

JustisTRACK provides risk notifications and network drawings on the entire network of natural persons, undertakings and legal persons involved in a legal person. This information is used to identify and analyse the risk of abuse of legal entities, for use by supervisors and LEAs. JustisTRACK can also provide knowledge and expertise on the abuse of legal entities and financial economic crime. Authorities—such as some supervisors, Tax and Customs Administration, LEAs, Customs, and the OM—can receive the TRACK reports.

Every year there are an average of 1.4 million changes in the company register of the CoC. These changes are the starting point of an investigation by JustisTRACK in the automatic analysis. On average there are approximately 400 000 changes that lead to a trigger in the system Radar annually. Ultimately, more than 2 000 of these signals are examined by a JustisTRACK analyst because they indicate enhanced risk of abuse of a legal entity. Indicators include involvement in bankruptcies or dissolutions, involvement of natural persons with antecedents, or multiple board changes or changes of address in a short period of time. An indicator on its own is never sufficient to identify a risk, but a signal is further examined when a combination of indicators is used.

473. Customer due diligence measures performed by obliged entities are also seen as a key mitigation measure in the prevention of the misuse of legal persons that are clients or related to clients of obliged entities. Obliged persons are required to identify and verify the identity of the client, including their BOs. The information required includes the nature of business and personal details of directors, and source of assets if necessary. Although obliged entities are not permitted to rely solely on the BO register to identify the BOs of their clients, almost all participants interviewed during the onsite mentioned the register as one of their main sources of BO information. In practice, the absence of a fully populated BO register makes it more difficult for obliged entities to identify and verify BOs, especially in the case of complex group structures, such as conduit companies. The AFM notes that its investigations into obliged entities show that they regularly fail to complete the identification and verification of the real BO for customers with complex legal structures.

474. A further weakness in the system is that notaries too often make use of the legal possibility to identify senior management as "pseudo BOs", rather than more rigorously assessing if there are no natural persons owning or controlling the legal person by other means, as part of their CDD when creating companies. This issue of excessive qualification and registration of senior management as pseudo-BOs by notaries has also been publicly flagged by the trust office sector, who have seen the persons they appointed to provide director services, registered as pseudo-BO.

475. Trust offices play an important role as a gatekeeper, particularly given that they service an important share of conduit companies and other customers that originate outside the Netherlands looking to set up a legal person in the Netherlands. Stricter regulation and supervision by DNB on trust offices since 2018 has led to an improved implementation of BO obligations by licensed trust offices. However a part of the trust sector has reacted by restructuring their business models to circumvent this stricter regulation and supervision, leading to an "illegal trust office sector" with an estimated marked share of 15%. These illegal trust offices are less likely to properly implement BO-obligations or report unusual transactions and are more likely to attract clients who want the BO of the structures they set up in the Netherlands to remain unknown.

476. The Dutch authorities recognise this problem and the Ministry of Finance is carrying out in-depth research on possible solutions. As well as undertaking some activities, such as the FEC project of Trust Offices (see 6.2) to mitigate these issues. In the interim, this remains a significant risk and the Assessment Team considers this to have an important impact on the effectiveness of the system. It also undermines confidence in licensed trust offices that fulfil their obligations and places them at a competitive disadvantage. DNB investigates signals it receives about illegal trust offices. In most cases, these signals are addressed through informal action such as warning letters and requests for information. Between 2016 and 2021, out of 82 investigated signals that led to interventions, only eight resulted in formal enforcement measures.

477. Private and public limited liability companies are required to keep a register of BOs and shareholders and beneficiaries of shares. Foundations must register all their beneficiaries internally. These requirements are not monitored so there is no way to determine the extent to which companies are compliant with this obligation. However, obliged entities are required to obtain this information as part of CDD process and provide it to LEAs when requested in a criminal investigation.

478. Bearer shares can no longer be issued in the Netherlands. A number of bearer shares remain in circulation, but the Dutch authorities are unable to quantify the exact number. Holders of existing bearer shares can still receive their registered shares if they present their former bearer shares to the issuing company before 1 January 2026. The authorities believe this is a low risk since the holder of the bearer shares has lost all rights under those shares. In addition, in 2018, the authorities estimated on the basis of research undertaken by the Tax and Customs Administration that only 75 public limited liability companies held bearer shares at that time.

BES Islands

479. The secretary of the commercial registry supervises legal persons' compliance with the BES commercial register obligations. The CoC Bonaire performs checks to make sure procedural obligations are met and may ask for further documentary evidence of the stated data. The CoC Bonaire contains a large number of sleeping companies due to the complexity of officially dissolving companies. As of 1 November 2021, the CoCs in the Caribbean Netherlands switched to a new IT system to improve the quality of the information in the commercial register.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

480. Relevant authorities generally have good access to basic information and sources of potential BO information on most types of legal persons created in the Netherlands; however, a fully populated BO register and a more rigorous implementation of BO obligations by obliged entities would significantly improve the quality and timely access to BO information. Basic information on legal persons is available online and instantly through the CoC company register. This information is publicly available upon the payment of a fee. Basic information is provided directly to the Tax and Customs Administration, JustisTRACK and the Statistics Bureau via a specialised service channel and some obliged entities, such as banks that have a direct technical link to the company register. The CoC regularly monitors this information through automated and manual verifications and an external auditor reviews a sample every three years. The most recent audit showed that 99% of authentic obligatory data is legally correct, meaning that all mandatory fields are filled with information that is consistent with the Personal Record Database, and the documents provided. This suggests a high level of accuracy, but does not guarantee that the data is up-to-date.

481. It is expected that the CoC BO register will become the central resource for accessing BO on most legal persons in a timely manner. As noted above, the register is currently only partially populated (27% complete as of November 2021).

482. Obliged entities are required to collect and maintain basic and BO on their customers and to verify this information against data held in the CoC BO register. This information can be requested by FIU-NL and Wwft supervisors or subpoenaed by competent authorities. The Dutch authorities explained that it is not common practice for this information to be requested in this way due to the fact that relevant information can often be retrieved via CoC and iCOV. The Assessment Team is of the opinion that, although CoC and iCOV may contain information on who the directors are or who declared the taxes of legal persons, this cannot be considered as adequate, accurate and current BO information. Furthermore, the accuracy of BO information held by obliged entities is unclear given the practice of too often settling for pseudo-BOs and the fact that many of the recent failings identified by AML/CFT supervisors relate to CDD (including incorrect BO information).

483. Almost all forms of legal persons are required to file annual tax returns with the Tax and Customs Administration. For public and private limited liability companies, this includes certain shareholder information, including the name, address, place and country of residence, as well as income and loss statements. However, due to their limited 'real' activities in the Netherlands (i.e., no or few employees and a low net turnover), conduit companies (often in the form of BVs) often have minimal financial reporting obligations – publishing only a limited balance sheet, without explanatory notes, profit and loss accounts, management report or auditor's reports – even though they hold large Foreign Direct Investment assets or significant financial incomes, such as interest income and equity capital gains.

484. The Dutch authorities presented case examples demonstrating that LEAs are able to identify (foreign) legal persons used in ML schemes, and prosecute and convict Dutch citizens involved in these schemes. However, the authorities encounter more difficulties in identifying the ultimate BO of complex legal structures, especially when foreign legal persons are involved. Investigative tools such as iCOV and JustisTRACK allow LEAs to quickly gather information from different sources that may contain indications of who is the BO of a legal person, but time is needed to analyse this information or to conduct further investigations in order to substantiate and confirm that the presumed BO is indeed the real BO.

BES Islands

485. Obliged entities in the BES Islands have the same requirements to obtain BO information as part of their CDD obligations. These obligations are supervised by competent authorities. Prior to 1 July 2021, BTWwft were not able to access civil-notary files to verify compliance with these obligations, and at the time of the onsite had still not done so. This is an area of concern given the role notaries play in high risk real estate transactions in the BES Islands.

486. The Dutch authorities have access to publicly available basic information on the company register. However, a subpoena is required for non-public information, which may reduce the ability of authorities to access this information in a timely manner.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

487. Open mutual funds that operate investment funds in the Netherlands are registered with the AFM and some basic information (such as fund manager and date of registration) is published on the AFM website. These funds are also registered with the Tax and Custom Administration, which holds information on the participants and beneficiaries that can be shared with competent authorities. Closed mutual funds, of which the shares/interests cannot be traded freely, are typically used to manage family assets. Although these funds are fiscally transparent (the assets are attributed to the settlor or similar person who will be subject to taxation), participants are not obliged to disclose their participation to the Tax and Customs Administration. Participants must disclose the holdings, even if managed in a closed fund, to the Tax and Customs Administration as part of their regular annual income tax return. Mutual funds can be created without intervention of a notary and as with foreign trusts and legal arrangements are not registered at the CoC.[63] Thus, competent authorities have access to information sources that contain potential BO information, but it is not always easy to understand the identity of the ultimate controller, particularly in a timely manner.

[63] Legislation to establish a BO register for legal and other similar arrangements is set up was adopted on the 24th November 2021 and will also include mutual funds.

488. It is not precisely known how many foreign legal arrangements are active in the Netherlands, but the authorities estimate up to 15 000. There are 1 173 foreign trusts serviced by Dutch trust offices. DNB is able to obtain information on these trusts (e.g. investments, country of establishment) via the trust offices. For those trusts that are not serviced by Dutch trust offices, LEAs must rely on international information sources or international co-operation to obtain basic or BO information of these legal arrangements.

BES Islands

489. Legal arrangements cannot be established on the BES Islands, with the exception of mutual funds. According to the Tax and Customs Administration there are currently no open mutual funds. There is no explicit prohibition of foreign trusts having activities in the BES Islands, however, there are no indications that this is occurring at a large scale in practice.

Effectiveness, proportionality and dissuasiveness of sanctions

490. The Netherlands has the ability to impose significant sanctions for failures to register changes to basic information and not maintaining BO information within the company register, including when it is done with intent. These sanctions can be applied to natural and legal persons and can result in prison sentences. At the time of the onsite, these powers have not been used in a meaningful way.

491. The Economic Enforcement Office (BEH) of the Tax and Customs Authority is responsible for detecting administrative violations relating to the company register. The BEH investigates signals of incorrect entries to the register and legal entities without any economic activity to the register from the CoC, Tax and Customs Administration and other sources. The BEH makes a recommendation of action to the CoC on the basis of its investigations. These recommendations usually call for deregistering the entity and relate to (intentionally) incorrect registration in the commercial register or because the legal entity is no longer active. Although the BEH can impose a penalty or cease and desist order, it has not done so to date even though there have been cases where false information was deliberately provided. This is not a proportionate use of sanctions and is a significant deficiency given the risk and context of the Netherlands as a financial centre.

492. Based on criteria set by the OM, the BEH also reports to the OM approximately 1 300 entities per year where registration violations pertaining to the obligation to file financial statements have been identified. This figure (1 300) is pre-agreed based on resource constraints, but usually BEH reports more legal entities to the OM (e.g., 1 750 in 2021). Sanctions in these cases have been imposed, but range between EUR 600 and 1 000. The Dutch authorities claim that these penalties correspond with other administrative offences and are considered high by the punished entities. Nevertheless, given the high number of remaining violations even after receiving a reminder (only a small percentage of violations are being sanctioned), the Assessment Team does not regard these sanctions as being dissuasive.

7

Overall conclusion on IO.5

1. The Netherlands has a good understanding of the risk posed by the misuse of legal persons and various authorities have undertaken different initiatives aimed at identifying and assessing the ML/TF risks of legal persons in certain sectors. However, there is no comprehensive view of the ML/TF risks related to the different types of legal persons.
2. There is currently no central source where LEAs can have timely access to adequate, accurate and current BO information on legal persons. In most instances, LEAs combine information found in open sources and information hubs such as JustisTRACK. Identifying BOs in a timely manner is hampered by the fact that, in some cases, information is held or registered about pseudo BOs (senior managing directors) and there is a lack of understanding by some obliged entities on how to identify the ultimate BOs when complex legal structures are involved.
3. Criminal sanctions imposed for failure to register or update information in the company register focus on failures by legal persons to file financial statements. Given the high number of violations, sanctions are not considered dissuasive. Sanctions for failure to keep the information company register accurate and up to date mainly focus on dissolving registered legal entities that are no longer economically active. For incorrect BO information, a cease and desist order and a penalty can be imposed, and in cases with intent, a police report will be sent to the OM for criminal sanctioning. At the time of the onsite, no serious violations have been discovered concerning BO registration.
4. There are several deficiencies in the BES Islands, including a lack of timely access to adequate, accurate and current BO information on legal persons. These deficiencies are weighted appropriately based on the risk and context of the BES Islands.
5. The Netherlands is rated as having a moderate level of effectiveness for IO.5.

Chapter 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

1. The Netherlands has a robust legal framework for all forms of international co-operation. International co-operation with foreign counterparts, particularly EU member states, is proactive, collaborative, and provided both upon request and spontaneously. There is, however, a minor technical deficiency related to the explicit legal basis for FIU-NL to provide co-operation to non-EU/EEA FIUs, but this does not significantly impact effectiveness.
2. The Netherlands seeks and provides timely and constructive MLA and extradition. While comprehensive statistics were not available, Netherlands provided sufficient case studies to try to demonstrate the timeliness of its MLA and extradition responses. Feedback from the FATF global network note that legal co-operation with the Netherlands is of high quality and timely. The vast majority of MLA requests (received and sent) are within the EU. Simplified procedures within the EU enhances co-operation with other member states in this regard. The Netherlands has active co-operation on asset recovery and confiscation, which was demonstrated by statistics and case studies.
3. The Netherlands' international co-operation efforts to tackle crime and threats involving VAs is particularly noteworthy, as demonstrated through case studies and presentations during the onsite visit. The Netherlands cooperates extensively and efficiently with foreign LEA counterparts, for example by exchanging technical expertise and contributing to foreign investigations.
4. LEAs, OM and FIU-NL effectively engage in other forms of international co-operation to share information, including financial intelligence. This includes participating in a range of international and regional bodies, bilateral co-operation on strategic issues and providing training and sharing best practices with other jurisdictions, for example on TBML. LEAs have a large network of liaison officers posted in countries prioritised according to crime risks, including ML and TF. Customs actively requests and provides information to/from EU and non-EU countries.
5. FIU-NL works bilaterally and multilaterally with counterparts. FIU-NL also shares relevant cross-border dissemination reports with other EU FIUs on an automated basis, in line with EU requirements. The number of cross-border dissemination reports by FIU-NL to its European counterparts is significant. Feedback from some EU Member States note that these type of reports could benefit from more context. However, FIU-NL provides further information and context to EU FIUs upon request.

6. The Netherlands initiates and takes part in Joint Investigation Teams (JITs). However, JITs cannot be established in the BES Islands and awareness among LEAs could be improved in terms of when JITs or other international co-operation tools are most appropriate.
7. Supervisors, LEAs, customs and other authorities cooperate efficiently with their foreign counterparts, notably financial supervisors provide and participate in special AML/CFT colleges. Other DNFBP supervisors and industry bodies focus less on international co-operation for sharing supervisory information, although some engagement with neighbouring countries, such as Germany and Belgium, does take place.
8. The Netherlands has several channels for obtaining basic and BO information. Foreign authorities have direct access to basic and some BO information for a small fee. However, at the time of the onsite the BO register was only partially populated and there was no direct access to basic information for legal entities in the BES Islands due to technical problems. Formal measures are in place to ensure non-public information can be obtained in a timely manner.

Recommended Actions

1. The Netherlands (as well as BES Islands) should continue to maintain and expand its registration of statistics on international legal assistance, including specific statistics for TF-related cases and asset tracing/seizure and confiscation. This should include information on timeliness in responding to requests, so that it can monitor effectiveness and make improvements where necessary.
2. FIU-NL should seek a dialogue on how the quality of cross-border dissemination reports between EU FIUs can further improve their utility by recipient FIUs from the EU.
3. The Netherlands should clarify in law the FIU-NL's explicit legal basis to cooperate and exchange information with non-EU/EEA FIUs.
4. DNFBP supervisors should engage more fully in international co-operation with their foreign counterparts.
5. The Netherlands should raise the awareness of LEAs on the use of Joint Investigative Teams (JITs) and when they are most appropriate, in order to enhance their ability to proactively seek assistance in complex cases, in line with ML/TF risks. The Netherlands should also amend its legislation so that LEAs in the BES Islands have the ability to establish JITs.
6. The BES Islands should ensure that its CoC databases are fully operational in order to facilitate timely access of basic information by foreign authorities.

493. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40 and elements of R.9, 15, 24, 25 and 32.

Immediate Outcome 2 (International Co-operation)

494. International co-operation is critical for the Netherlands given its position as a global financial centre, transportation hub and the risks it faces as an origin, transit and destination country for the production and trafficking of drugs (see Chapter 1). The Netherlands considers international co-operation an integral part of its domestic legal framework. It has developed a network of dedicated experts and organisations to work closely together and lend their services internally as well as externally. The Netherlands engages in a wide variety of international co-operation, including on major international cases involving VA (see Boxes 3.9 and 8.3). The Netherlands actively seeks and provides informal and formal assistance for cases involving a transnational element, including during the intelligence phase, aided by an overseas LEA liaison network. The Netherlands provides MLA and extradition in accordance with the requirements set out in international treaties and domestic legislation (see R.36-39) and prioritises these accordingly.

Providing constructive and timely MLA and extradition

495. The Netherlands provides timely and constructive responses to MLA and extradition requests. Responses received by the FATF global network indicate that the provision of MLA is of high-quality, and properly prioritised. Simplified procedures within the EU enhance co-operation with EU member states, which account for the vast majority of the Netherlands' MLA requests. There is active co-operation on asset tracing and confiscation. This assessment was based on limited statistics; case studies; feedback from FATF and FSRB delegations; and interviews with relevant Dutch authorities.

Mutual Legal Assistance

496. The Department of International Legal Assistance in Criminal Matters (AIRS) of the Ministry of Justice and Security is the central body for the assessment of MLA requests to and from countries outside the EU. AIRS has clear domestic processes and communication guidelines for registering and executing MLA extradition and surrender requests, executing transfers of criminal proceedings and enforcing criminal sentences. The decision to seek MLA is typically taken by the OM.

497. The procedure for executing MLA and extradition requests [including European Arrest Warrants (EAWs), Investigation and Freezing Orders (EIOs)] depends on whether the co-operation is with an EU or non-EU member state. MLA requests from countries outside of the EU are sent through AIRS and then dispatched to the relevant International Legal Assistances Centres (IRCs) in the Netherlands. An IRC is an OM and LEA co-operation team and consists of one or two prosecutors, assistants to the prosecutor, administrative staff and police officers, who work together on MLA requests. The close co-operation between LEAs and prosecutors on judicial MLA requests enhances the efficiency of the system. Requests from EU member states, including EAWs and EIOs, are sent directly to an IRC.

498. The National Uniform Registration System for International Legal Assistance in Criminal Matters (LURIS), is used for all incoming MLA requests, regardless of whether they are received directly by the IRC or received first by AIRS. LURIS, established in 2002, is managed by the Judicial Information Service, and facilitates the timely execution of international requests through system alerts. A new case management system with similar functionality, the Dutch International Assistance System (DIAS), is soon to be introduced and will mitigate information security concerns identified in the outdated LURIS system.

499. The total number of MLA requests received by continental Netherlands is steadily rising. Between 2016 and 2021, the Netherlands received 23 373 judicial MLA requests related to terrorism, ML, drug crimes and fraud. As indicated in the table below, MLA requests experienced a slight decrease in 2020, coinciding with the start of the global COVID-19 pandemic. Incoming judicial MLA requests for ML represent 8.8% of all reported incoming requests. The offence of TF is not included as a separate offence in the LURIS system, therefore the Dutch authorities are unable to provide any MLA figures on TF alone. Moreover, the authorities only reported MLA statistics for two predicate offences—drug crimes and fraud—as more than 90% of all proceeds of crimes involve these two offences. Therefore, the shortfall in statistics do not relate to areas of high risk in the context of the Netherlands. With regard to non-EU countries, all MLA requests concerning asset recovery are also registered in the LURIS system. The LURIS system is unable to filter these requests from other MLA requests.

Table 8.1. Incoming judicial MLA requests for ML, TF, drug crimes and fraud

	2016	2017	2018	2019	2020	2021*	Total
European Investigation Orders for terrorism	N/A	13	32	30	21	27	123
MLA for Terrorism (including TF)	54	44	21	25	29	41	214
Total for Terrorism	*54*	*57*	*53*	*55*	*50*	68	337
European Investigation Orders for ML	N/A	35	199	305	303	374	1216
MLA for ML	126	134	80	120	118	99	677
ML (MLA other)	9	10	16	28	36	56	155
Total for ML	*135*	*179*	*295*	*453*	*457*	529	2048
European Investigation Orders for Drug Crimes	N/A	218	632	624	625	481	2580
MLA for Drug Crimes	1225	1047	802	735	823	846	5478
Drug Crimes (MLA other)	80	70	57	71	82	82	442
Total for Drug Crimes	*1305*	*1335*	*1491*	*1430*	*1530*	1409	8500
European Investigation Orders for Fraud	N/A	294	945	1357	1279	1281	5156
MLA for Fraud	1704	1480	758	503	540	308	5293
Fraud (MLA other)	200	227	387	455	355	415	2039
Total for fraud	*1904*	*2001*	*2090*	*2315*	*2174*	2004	12488

Note: “MLA” includes all MLA requests that involve some kind of investigative measure that are not EIO, also Prum DNA requests, request for European evidence warrant until 21/02/2016.
“MLA other” includes requests for transferring criminal proceedings, requests for European protection order, requests for European supervision order, notification interception Annex C, transfer of criminal proceedings and transit requests
“Fraud” entails forgery (ex Article 225 WvSr), deceit (Article 326 WvSr embezzlement (Article 321) WvSr, tax fraud (Article 68, Article 69 and Article 69a General Act pertaining to national taxes)
*Covers the full year of 2021

500. FATF jurisdictions that provided input related to the provision of MLA by Dutch authorities for ML/TF-related cases reported, in general, a high level of co-operation and quality responses, including on the timeliness of responses. Incoming MLA requests (and other legal requests) primarily originate from EU member states (85% of all incoming requests). Within the EU, most requests came from Belgium, Germany, France, and Poland. Outside of the EU, the most frequent incoming requests originate from the United Kingdom, Switzerland, Turkey, the United States and Norway.

501. The Dutch authorities do not maintain clear statistics to demonstrate the timeliness of executing MLA requests in practice. The Ministry of Justice's internal guidelines state that incoming MLAs should be handled within five working days, and outgoing MLAs within three working days. When a concrete timeframe is mentioned in the MLA request, the AIRS contacts the IRC to make sure the request has been executed. If no time frame is stipulated, AIRS contacts the IRC within six months upon receipt of the request.

502. Timeframes are faster under the EIOs regime, as they are set out in European law (must be executed within 90 days following recognition, with a possibility to extend by a maximum of 30 days). However, the authorities also do not maintain clear statistics on EIOs, and are therefore unable to demonstrate what the timelines are in practice. The authorities state that urgent requests can be processed within a matter of days.

503. On average, the Netherlands reports that 20 MLA requests per year are denied because of dual criminality or incompleteness. One of the main types of crime for which no dual criminality exists relate to scam cases.

504. The Netherlands also provides a range of assistance for asset recovery, including identifying, tracing, seizing and confiscating assets. A request from a foreign country may be made by means of a European asset freezing order (if an EU member state). If the assets are outside the EU or there are reasons not to issue an asset freezing order, for example the complexity of the case, application for legal assistance is made through an MLA request. The Netherlands maintains statistics on pending MLA requests registered since 2016. The Netherlands does not maintain statistics on MLA requests with regard to the seizure of assets. Moreover, the LURIS system does not make a distinction between requests concerning the seizure of evidence and the seizure of proceeds of crime. There are currently 335 pending MLA requests since 2016, including the seizing of assets or the levying of a prejudgment seizure. These requests may include multiple objects and assets to be seized. This number includes requests in which the (prejudgment) seizure was imposed but the case was not yet finalised. Statistics on the number of finalised/executed MLA requests are not available. The Netherlands provided the below case study to demonstrate the timely response to a MLA request for seizure of property related to a foreign ML investigation. In this example, the seizure took place on the same day that the MLA request was received.

Box 8.1. Seizure of a vessel upon a foreign MLA request

In December 2016, the Swiss authorities requested urgent assistance in freezing an expensive yacht docked in the Netherlands. The yacht was worth EUR 100 million, and supposedly belonged to the son of the President of an African country, who was under investigation for corruption and ML. The Netherlands established a multidisciplinary team to execute promptly the Swiss request. They established the legal ownership of the vessel, which was registered under the Cayman Islands flag and under the name of a limited company established in the Marshall Islands. Through open source information, they linked the vessel's ownership to the suspect. On the same day of the MLA request, the police seized the yacht. The Dutch authorities also found a proper location to store the yacht, and the Swiss authorities registered the seizure on the Cayman Islands. The Netherlands and Switzerland reached an agreement to share the costs related to the maintenance of the vessel. The Swiss authorities reached an out of court settlement with the suspect and lifted the seizure.

505. Incoming and outgoing EU freezing orders and final EU confiscation orders (relating to ML/TF/predicate offences) are annually reported to the EC. Therefore, the Netherlands provided more detailed statistics on these EU orders, as compared to finalised MLA requests. As evidenced in the table below, the Netherlands makes regular use of the EU freezing and confiscation order regime.

Table 8.2. Incoming and outgoing EU freezing and confiscation orders

	2017	2018	2019	2020
European Freezing Orders received	6	22	28	55
European Freezing Orders sent	32	40	68	96
Final European Confiscation Orders - received	22	26	30	30
Value*	€ 126 665	€ 5 188 652	€ 513 435	€ 574 054
Final European Confiscation Orders - sent	20	17	20	19
Value*	€ 27 843 057	€ 10 471 490	€ 124 076	€ 462 248

Note: *Estimated Value of the assets that have been confiscated at the time of the Confiscation Order

506. No statistics are maintained as to the number of requests on asset sharing and recovery of proceeds involving foreign predicate offences or proceeds moved to other countries. However, the Netherlands provided a case study (see Box 3.17 under IO.8) to demonstrate its effectiveness in asset sharing with foreign counterparts.

507. A European asset freezing order is transmitted through an IRC directly to the competent foreign authority, which only needs to recognise and execute the order. If further information is needed before the asset freezing order is transmitted, for example about registration in a foreign register, it can be obtained quickly through an Asset Recovery Office (ARO) request. IRCs can ask the judicial ARO for assistance, and can call upon the expertise of accountants, asset tracers, civil law advisers and the Asset Management Office, as well as specialised prosecutors and assistants to the prosecutor. Both the police ARO and the judicial ARO are connected to, and makes use of, the CARIN network.

508. The below table summarises the number of ARO requests and sent and received since 2017. As indicated below, the Netherlands sends more ARO requests than it receives, and the number of requests is largely static between 2017 and 2020.

Table 8.3. Number of judicial ARO requests

Year	2017	2018	2019	2020
Incoming requests	114	108	111	162
Outgoing requests	437	392	333	397
CARIN	1	12	18	19
Total requests	552	512	462	578

509. Different timeframes are set for the execution of ARO requests: eight hours for urgent requests, one week for non-urgent requests if the requested information is held in a database directly accessible by the LEA and in case the crime is mentioned on the list of Council Framework Decision 2006/960/JBZ, and 14 days for all other cases. The Netherlands does not maintain statistics on the average timeframes met to respond to ARO requests in practice, but notes that delays are rare.

510. The international transfer of sentences is governed by two acts: the WETS (for EU member states) and the WOTS (for non-EU countries). These acts apply to Dutch citizens and foreign prisoners in the Netherlands and Dutch prisoners abroad. The WOTS and the WETS allow for an international transfer and enforcement of a foreign sentence in a criminal case. The transfer of sentences falls under the responsibility of the Minister of Justice and Security. The below table summarises requests received and answered by the Dutch authorities between 2016 and 2021, which primarily concern drug crimes as the underlying predicate offence. Of these figures, two incoming requests pertained to TF and seven to ML.

Table 8.4. Incoming WETS and WOTS successful requests

	2016	2017	2018	2019	2020	2021*	Total
All incoming WETS requests (EU)	237	274	253	314	260	224	1562
All incoming WOTs requests (non-EU)	98	56	32	37	15	9	247
Total	335	330	285	351	275	233	1809

Note: covers the period up to October 2021.

511. Joint Investigation Teams are used in complex international criminal cases where applicable and comprise of a legal agreement between competent authorities of two or more states for the purpose of carrying out joint criminal investigations. An MLA request is always used for the establishment of a JIT, which must be registered in LURIS by the IRC where the request is received and sent to the OM. Requests to *participate* from EUROJUST, EUROPOL or European Anti-Fraud Office must also be sent to the national IRC. Between 2016 and 2020, the Netherlands received a total of 15 requests for co-ordination meetings from EUROJUST on whether to establish JITs. The Dutch authorities do not maintain detailed statistics on the number of JITs established based on these co-ordination meetings. However, the below case study demonstrates the Netherlands' effectiveness in contributing to JITs upon request.

Box 8.2. JIT leading to arrests and seizures across several jurisdictions

On 21 November 2016, a JIT was established to investigate a ML ring moving the proceeds from drug trafficking Europe to Morocco via the Middle East. Unregulated financial channels (the hawala system) were used to move the proceeds from this activity, which were estimated to amount to over EUR 300 million. The work of the JIT led to the arrest of 36 suspects in France, Belgium and the Netherlands. Following the arrests, over EUR 5.5 million in cash, EUR 800 000 in gold and two semi-automatic weapons and ammunition were recovered.

Extradition

512. The Netherlands has two types of extradition processes: accelerated and normal. If the person consents to extradition, the accelerated procedure can be followed, which means that the person sought will be extradited immediately without any court proceedings. The normal procedure is primarily handled by the district court and takes approximately three to six months. However, this also depends on whether an appeal is lodged. If the extradition request is made under the EAW, the court in Amsterdam is the central authority to decide on the request. As noted in R.39, the Netherlands allows the extradition of Dutch nationals (under certain conditions), even outside the EU framework. The below table summarises all incoming extradition requests received during the assessment period. The case management system LURIS does not distinguish between extradition requests or international alerts issued for wanted persons. Therefore, the number of actual extradition requests is lower than illustrated in the below table.

Table 8.5. Incoming extradition requests (including international alerts for wanted persons)

	2016	2017	2018	2019	2020	2021*	Total
Extradition							
ML	3	2	7	5	1	2	20
Terrorism (including TF)	20	10	12	16	18	11	87
Drug Crimes	26	36	27	41	27	39	196
Fraud	17	15	17	24	27	18	118
European Arrest Warrants							
ML	6	5	2	1	3	2	19
Terrorism (including TF)	3	0	1	3	0	0	7
Drug Crimes	196	134	69	42	17	35	493
Fraud	78	32	48	6	6	4	174
Total	349	234	183	138	99	41	1044

*Covers the full year of 2021

513. As indicated in the above table, the total number of EAW extradition requests has decreased since 2016. Most requests relate to drug-related crimes, which is in line with the Netherlands' risk profile. AIRS requires that extradition requests should be processed in accordance with legal time limits in relation to provisional arrest, and the initiation of judicial proceedings. No statistics, or case studies occurring during the assessment period, were presented to demonstrate that these timelines are followed in practice.

514. The Netherlands does not maintain detailed statistics on the percentage of extradition ML/TF requests acceded, but states that the majority of requests are executed. The authorities state that the most frequent reason to deny an extradition request is due to the lack of a treaty or dual criminality, or for administrative reasons (e.g., such as double registration or withdrawal by requesting countries). From 2018-2021, a total of 6 434 extradition requests were received for all crimes. From those requests:

- 168 Europeans Arrest Warrants were denied without an underlying reason provided;
- 148 were withdrawn by the requesting country;
- four were denied based on a lack of dual criminality;
- one was denied on the basis of *ne bis in idem.*[64]

515. Regarding the timeframes for executing arrest warrants, the timelines are set out in European law and a decision must be made no more than 60 days following the arrest of the person sought. Authorities indicated that most EAW requests are executed within these timeframes. Given the EU framework, a warning is sent when timelines are exceeded. The Netherlands has never received such a warning.

[64] Whereby a person cannot be punished and subjected to several procedures twice for the same facts.

BES Islands

516. The Prosecutor's office of the BES island is part of the Prosecutor's Office Carib (OM Carib, together with Curacao and Sint Maarten Aruba has a separate prosecutor's office) and this influences the execution of MLAs. The OM Carib has its own IRC, the IRC Carib (Aruba excluded though there is close co-operation between IRC Carib and Aruba). The IRC Carib functions as the Central Authority for the countries of Curacao and Sint Maarten, whereas the Central Authority for MLA for the BES Islands is in continental Netherlands. Within the Kingdom, MLAs from the Netherlands to BES Islands are categorised as interregional MLAs, as are MLAs from and between Curacao, Sint Maarten, Aruba and BES Islands. Within the Caribbean region, the BES Islands receive the most MLAs from Aruba, Curacao and Sint Maarten.

517. In regard to the BES Islands, incoming and outgoing MLA requests (and other legal requests) to and from non-EU member states are executed through AIRS, which subsequently transmits the request to OM Carib. MLA requests from/to EU member states, including continental Netherlands, are sent and received directly via IRC Carib. The IRC Carib then submits the request to the IRC OM in Bonaire, who further assigns them to the Police. The IRC Carib uses its own numbering and a manual system to register and monitor MLA requests, which is not connected to the LURIS system.

518. The total number of incoming MLA requests for the BES Islands from 2017 to 2020 is 74, with most requests originating from continental Netherlands, followed by the United States, and involve ML, asset recovery and homicide. These requests are mostly minor requests, not relating to extradition. One extradition request was submitted in the assessment period but did not relate to ML or TF. Insufficient information was provided on the time frames of the execution of the requests.

519. As noted in the TC Annex (see R.40), JITs cannot yet be established in the BES Islands.[65]

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

520. Outgoing MLA requests from the Netherlands to foreign countries operate under the same system as incoming requests. Therefore, all structures, procedures and instruments used above apply equally for outgoing MLA requests.

Mutual Legal Assistance

521. The Minister of Justice and Security is ultimately responsible for sending MLA requests to countries outside the EU, particularly with non-treaty countries. In these cases, AIRS, on behalf of the Minister of Justice and Security, assesses whether it is possible or desirable to make an MLA request to a non-treaty country. If necessary, AIRS may consult MFA and LEA liaison officers posted in that country before filing the MLA request.

65 At the time of writing, the Code of Criminal Procedures for the BES Islands is being modernised. Although it is unclear to what extent the JITs will be used by the BES, given the proportion and size of the BES Islands, the modernisation will include a legal basis for establishing JITs in the BES Islands.

522. During the onsite, Dutch authorities emphasised the importance of seeking international co-operation in the intelligence phase before and during ML and TF investigations, as nearly all ML cases include a transnational element. Furthermore, there is strong domestic co-operation in place on international co-operation matters, including between law enforcement and judicial authorities. For instance, there is a standing consultation structure in which the IRCs, AIRS and other stakeholders meet to discuss operational problems and exchange expertise related to MLA. These meetings are chaired by the national IRC and take place approximately five times a year.

523. In general, MLA requests sent abroad take considerable time to be responded to, even with reminders sent every few months. With regard to EOIs, it is expected that the time limits, as stipulated by EU law, are respected by the requesting state. AIRS is responsible for tracking all outgoing MLA requests.

524. Most (75%) outgoing MLA requests are sent to EU member states. Within the EU, requests are primarily sent to Belgium, Germany, Poland, Spain and France. Outside of the EU, the Netherlands most frequently sends MLA requests to the United States, Turkey, Surinam, Switzerland and Morocco. During the period between 2016 and 2021, a total of 4 765 outgoing MLA requests concerning ML or terrorism were registered. The percentage of outgoing MLA requests related to ML (33.6%) is significantly higher than incoming ML MLA requests (8.8%). Similar to incoming requests, the Netherlands does not maintain statistics on TF MLA specifically but as with incoming MLA requests, there appear to be significant increases in outgoing MLA requests between 2020 and 2021 for some categories including MLA for terrorism (including TF). The reason for this is not clear to the Assessment Team.

Table 8.6. All outgoing judicial MLA requests

	2016	2017	2018	2019	2020	2021*	Total
European Investigation Orders for TF	N/A	26	39	49	25	25	164
MLA for Terrorism	69	46	18	20	11	23	187
MLA other for Terrorism	2	0	0	1	0	0	3
Total for Terrorism	*71*	*72*	*57*	*70*	*36*	48	354
European Investigation Orders for ML	N/A	244	539	481	458	437	2 159
MLA for ML	507	449	341	316	282	296	2 191
MLA other for ML	6	4	9	21	10	25	61
Total for ML	*513*	*697*	*889*	*818*	750	598	4 411
European Investigation Orders for Drug Crimes	N/A	207	392	413	391	346	1 749
MLA for Drug Crimes	1160	524	409	373	226	227	2 919
MLA other for Drug Crimes	14	9	1	29	28	25	106
Total for Drug Crimes	*1 174*	*740*	*802*	*815*	*645*	598	4 774
European Investigation Orders for Fraud	N/A	167	368	298	318	311	1 462
MLA Fraud	439	435	316	377	203	242	2 012
MLA other for Fraud	18	15	4	29	22	24	112
Total for Fraud	*457*	*617*	*688*	*704*	*543*	577	3 586

Note: MLA includes all MLA requests that involve some kind of investigative measure that are not EIO, also Prum DNA requests, request for European evidence warrant until 22/02/2016.

MLA "other" includes requests for transferring criminal proceedings, requests for European protection order, requests for European supervision order, notification interception Annex C, transfer of criminal proceedings and transit requests.
"Fraud" entails forgery (e.g., Article 225 WvSr), deceit (Article 326 WvSr embezzlement (Article 321 WvSr, tax fraud (Article 68, Article 69 and Article 69a General Act pertaining to national taxes).
*Covers the full year of 2021

525. Outgoing requests with regard to establishing a JIT are registered with the IRC and approved by the Board of Prosecutor General. The OM is responsible to develop a plan of action with the competent authorities of the participating countries. A request to establish a JIT (with another EU member state) may be supported by EUROJUST. For example, the Netherlands can forward initiations of a JIT to EUROJUST, with a view to use the wider network of specialised LEAs in Europe. During the assessment period, a total of seven JITs related to ML were established at the request of the Netherlands. During the onsite interviews, it was noted that LEAs would prefer to have more JITs established, where relevant, as almost all ML investigations in the Netherlands include transnational elements. However, generally, there appear to be divergent views within the Netherlands on when JITs are the most efficient and practical way to cooperate in transnational criminal cases and some representatives felt other mechanisms are more appropriate in some of the cases where JITs are proposed. Due the divergent views, the Assessment Team believes that the Netherlands should provide specialised and systematic training in the use of international co-operation tools, including JITs, and further develop circulars and other facilitative material for personnel dealing with extradition and MLA and to enhance their ability to proactively seek assistance in complex cases, in line with the Netherland's ML/TF risk profile. Regarding the international transfer of sentences, the Netherlands reported 986 requests to transfer sentences as outlined in the table below.

Table 8.7. Outgoing WETS and WOTS requests

	2016	2017	2018	2019	2020	Total
All outgoing WOTS requests (EU)	19	73	54	26	31	203
All outgoing WETs requests (non-EU)	132	134	135	189	193	783
Total	151	207	189	215	224	986

Extradition

526. During the period between 2016 and 2021, a total of 2 133 outgoing extradition requests and EAWs were registered relating to ML, terrorism and the predicate offences related to drug crimes and fraud. As indicated in the table below, the Netherlands actively utilises both processes, making approximately 350 requests per year via the EAW system and approximately 18 per year to non-EU jurisdictions.

Table 8.8. Outgoing extradition and surrender requests concerning terrorism and ML

	2016	2017	2018	2019	2020	2021*	Total
Extradition							
ML	2	3	1	2	5	4	17
Terrorism (including TF)	4	3	1	2	5	0	15
Drug Crimes	11	14	6	13	8	14	66
Fraud	3	1	1	2	5	1	13
European Arrest Warrants							
ML	23	52	49	68	66	58	316
Terrorism (including TF)	199	17	18	222	3	0	459
Drug Crimes	135	121	133	182	178	137	886
Fraud	52	56	83	67	56	47	361
Total	429	267	292	558	326	261	2 133

Note: The Netherlands does not maintain statistics on TF extradition cases. These are included in the category of "terrorism".
* Covers the full year of 2021

BES Islands

527. The BES Islands have cooperated with authorities of other countries in various criminal investigations in recent years. For instance, five MLA requests were sent to countries outside Europe. In the period May 2017 to May 2020, a total number of 111 MLA requests were sent by the BES through IRC St. Maarten, with the largest percentage of requests sent to Aruba, Curaçao and Sint Maarten. During the period of the evaluation no outgoing extradition request was sent to continental Netherlands.

Seeking other forms of international co-operation for AML/CFT purposes

528. Competent authorities actively seek non-legal forms of international co-operation for AML/CFT purposes, particularly from European counterparts. The FIU-NL actively seeks input via the Egmont Group. At the supervisory level, a number of initiatives were taken by the Netherlands, primarily at the EU level. At the LEA level, various Dutch authorities have deployed liaison officers abroad which may seek international co-operation on behalf of the Netherlands but also provide information and expertise when possible. All efforts by LEAs and supervisors are aimed at contributing to effective foreign co-operation on combatting both ML and TF.

529. FIU-NL attaches great importance to foreign co-operation, for which it has built an extensive network. FIU-NL actively focusses on foreign co-operation with its FIU counterparts, both in Europe and worldwide, at an operational and strategic level. This co-operation focuses on sharing and obtaining information for the interpretation of transactions. Strategic co-operation is aimed at exchanging information as efficiently and effectively as possible. While the Assessment Team notes a minor technical deficiency under R.40 with regard to the explicit basis of FIU-NL to exchange information with non-EU/EEA FIUs, in practice FIU-NL shares information with all FIUs that are members of the Egmont Group. FIU-NL has

concluded 29 MoUs with foreign FIUs, where this is required by the foreign partner. The FIU-NL cooperates most with European FIUs through the EU FIU Platform. The below table summarises the number of outgoing FIU-NL requests for international co-operation sought from foreign counterparts on ML/TF matters. FIU-NL seeks most co-operation with FIUs from Germany, Belgium, Spain, the UK and Turkey.

Table 8.9. Number of outgoing FIU-NL requests

Year	No. of outgoing requests	No. of foreign FIUs involved
2021*	487	73
2020	590	85
2019	501	79
2018	543	76
2017	824	86
2016	827	84

* Covers the period up to 18 November 2021.

530. The FIOD, Police, KMar, and OM also maintain contacts with their foreign counterparts. All parties also make use of an extensive liaison officer network, with approximately 48 liaison officers posted in strategic countries and regions and is steadily growing. These contacts are used in investigations and for the exchange of knowledge and expertise. The Netherlands does not maintain statistics on informal requests for co-operation via its liaison officer network. The below case study was provided to demonstrate co-operation by Dutch authorities with foreign counterparts to seize more than EUR 25 million in VAs. This case demonstrates how the Netherlands effectively exchanges information with international counterparts, and also leverages this information to pursue investigations and prosecutions.

Box 8.3. Seizure of VAs

In 2019, all servers of Bestmixer, a VA mixing service based in the Netherlands and Luxembourg, were seized including user data, such as IP and email addresses. This information was shared through Europol and has led to several criminal investigations in various countries.

Since 2020, Dutch LEAs have cooperated on the analysis of financial information used through encrypted communication. Based on this data, a significant amount of wallets, including those linked to accounts at VASPs, have been criminalised (thereby allowing for confiscation proceedings). Dutch LEAs were then able to seize the funds in these accounts (EUR 25 million) and additional information on the users and their transactions were collected. This information was actively shared with other relevant jurisdictions. These cases are still under investigation.

531. LEAs also participate in a number of international bodies to seek and provide information to facilitate their criminal investigations and to trace and seize/confiscate assets. The main international bodies include: EUROPOL, INTERPOL, EUROJUST, EMPACT, and the CARIN and ARO networks. The Netherlands provided case studies demonstrating its exchange of information via these international bodies.

532. LEAs also use FCInet, a decentralised computer system that allows for searching and matching data between participating countries by financial criminal investigation services. FIOD, together with the UK's HM Revenue and Customs, is responsible for FCInet since 2016. For over five years, the Netherlands has invested in FCInet, which is GDPR compliant, to ensure expeditious and secure data insights for financial investigations. The advantage of FCInet is that the system includes data normally inaccessible to foreign LEAs, but enables partners to identify relevant data in line with privacy or data autonomy requirements. It is an intelligence instrument and while there are no specific statistics on how many investigations are based on information sought through this platform, the Dutch authorities state that they use this platform as a standard tool.

533. All LEAs can also receive information requests directly from their foreign police counterparts, in addition to receiving MLA requests through IRCs. If a so-called police-to-police request is made for information involving the use of coercive measures, the request must be forwarded to the OM. Requests must also be forwarded to OM if special investigative powers must be exercised or if the information obtained is to be used as evidence abroad. In these cases, the IRC structure is directly involved. Between 2016 and 2020, a total of 6 969 incoming police-to-police requests concerning ML or terrorism were registered.

534. During the period between 2016 and 2020, a total of 28 560 outgoing police requests were sent by the Dutch Police to their foreign counterparts, of which 1 262 concerned terrorism, and 2 676 included ML.

Box 8.4. Police-to-police co-operation: COVID-19 Fraud

On 24 February 2020, a police-to-police message was received via Interpol by the LIRC from the authorities in Hong Kong, China. A payment was made by a company in Hong Kong, China to a Dutch account related to the purchase of facemasks. The facemasks were not delivered and communication halted after the payment was completed. On 25 February 2020, the Interpol message was forwarded to the judicial ARO and IRC. Without a formal judicial request for legal assistance from the authorities in Hong Kong, China (which would have taken too much time), Dutch authorities could not freeze the Dutch account pursuant to Dutch law. Accordingly, the Dutch authorities commenced an ML investigation and restrained the Dutch account on the same day (25 February 2020). In close communication with foreign authorities and the bank, the restrained amount was returned to the account in Hong Kong, China.

535. Customs also requests information from EU and non-EU countries. Between 2015 and 2020, 100 requests were sent by Customs to its foreign counterparts. Customs also requests information on seized and forfeited cash through the European Customs Information System (CIS). Since 2016, Customs has transferred 247 cases related to CIS notification to FIOD/Kmar for ML investigations (see IO.8).

536. The Netherlands has a solid structure to co-operate internationally on asset recovery matters. As previously noted, the police ARO acts as special contact point for police-related asset confiscation, notably being requests for information, and received a total of 578 incoming and outgoing requests related to information on asset freezing and confiscation in 2020.

537. DNB and AFM both participate with their international counterparts on AML/CFT supervision. At a policy level, both supervisors are involved in several international fora such as the Basel Committee on Banking Supervision, the European Securities and Markets Authority and the EBA.

538. DNB and AFM also participate in the EBA AML Standing Committee. This Committee is composed of high-level representatives of all AML/CFT competent authorities. The Committee, which convenes approximately every eight weeks, facilitates and fosters the co-operation of competent AML/CFT authorities in the financial sector across the EU. Both supervisors also have a co-operation agreement with the ECB, which is involved in supervising the large banks under the Single Supervision Mechanism. For non EU member states, DNB and AFM mainly rely on MoUs for information sharing and co-operation. DNB has over 50 agreements covering a range of regions and the AFM is a signatory of the IOSCO multilateral MoU agreement. DNB shared or received information in 2019 (five occasions), in 2020 (13 occasions) and in 2021 (23 occasions) via bilateral contacts or information requests with other supervisory authorities outside of the Netherlands.

539. In addition, the Netherlands provided a number of case studies, such as one involving co-operation where formal measures were imposed on a FI with the headquarters in the Netherlands, with a subsidiary in a third country; as well as examples of working with other supervisors of entities with agents in the Netherlands.

Box 8.5. MVTS with a foreign license active in the Netherlands through notified agents

DNB conducted on-site examinations to an MVTS provider with a license in another EU country that was active in the Netherlands through a branch office and a network of registered agents. During the examinations, DNB established that customer identification data was incorrectly recorded in several customer files and other aspects of CDD were not being conducted. The on-site examinations at the branch office and the agents revealed that none of the entities verified the origin of the funds and the purpose and nature of customers' transactions. Other issues related to not filing UTRs and staff not being trained on their obligations. Following several meetings with representatives of the institution's head office abroad, the branch office and the agents, DNB in 2018 ordered the institution to set up a remedial programme to resolve the shortcomings, and to cease its activities until that had been completed. The outcome of the investigation and information on the board members of the MVTS provider was shared with the country authorities, who took action and after some consideration revoked the license in 2019.

540. DNB regularly organises and participates in international events including supervisory colleges. For example, in 2019 DNB organised the first AML/CFT college of supervisors of a Dutch FI that operates in several European Countries. In 2020, DNB organised AML/CFT supervisory colleges for three FIs and in 2021 organised AML/CFT supervisory colleges for ten FIs. Furthermore, in 2020, DNB participated in seven AML/CFT supervisory colleges and 29 AML/CFT supervisory colleges in 2021 by foreign AML/CFT supervisory authorities organised for FIs operating cross-border (including in the Netherlands). DNB has also developed and provided training and technical co-operation in recent years in order to share knowledge and experience with various foreign supervisors within the context of AML/CFT supervision. Furthermore, for the purpose of sharing knowledge and co-operation in the area of AML/CFT, DNB seconds staff members to foreign supervisors of international organisations.

541. At present the AFM hosts six supervisory colleges, and participates in a number of supervisory colleges. Moreover, between 2016 and 2020, AFM exchanged information related to cross-border ML cases (as well as other forms of financial crimes) on 51 occasions. No case studies were provided to demonstrate effectiveness in this regard.

BES Islands

542. FIU-NL performs the functions in continental Netherlands and the BES Islands and cooperates and provides information to its foreign counterparts in the same way it does for the continental Netherlands. Moreover, FIU-NL also cooperates internationally with regard to the Dutch Caribbean by using FCInet and by taking part in several meetings together with the FIUs of Aruba, Curacao and St. Maarten. Together with other FIUs in the Caribbean, FIU-NL also drew up a Kingdom Risk Analysis, based on a comparison of available information on reports of UTRs from the different FIUs in the Kingdom.

543. Law enforcement agencies in the Netherlands also exchange information and provide co-operation on behalf of the BES Islands. For example, KMar works with the United States on issues specific to the region and LEAs at the BES co-operate very closely together on non-legal issues as well.

544. The Customs Caribbean Netherlands is responsible for international co-operation with other jurisdictions as it relates to customs. This is facilitated by the Convention establishing the Caribbean Customs Organisation. However, this Convention was only established in 2019 and there is no information available on incoming and outgoing requests for co-operation before or after this Convention came into force.

545. DNB cooperates with the central banks of Curacao and Sint Maarten and Aruba and participates in the Board of Kingdom Supervisors, together with those central banks and the AFM. This co-operation includes harmonising to the largest extent possible with the AML/CFT laws and policies on the islands, sharing information on specific AML/CFT supervision cases that have a link with one or more of the islands and sharing information on fit and proper testing of policy makers active in FIs that are active on one or more of the islands.

8

Providing other forms international co-operation for AML/CFT purposes

546. The Netherlands is committed to increasing and strengthening networks for *providing* international co-operation for AML/CFT purposes. The different authorities play an active role in initiatives and projects aimed at doing so at the European and international level. For example, financial investigation was a key priority for the Dutch Presidency of the EU in 2016 and resulted in several initiatives and projects, which included strengthening co-operation between member states in order to deliver better financial investigation results. The Netherlands is also heavily involved in a range of other forums, such as the Global Coalition against ISIS, and co-leads the Global Counterterrorism Forum's Foreign Terrorist Fighters Working Group (FTF-working group). Amongst other examples of international engagement, in 2017, the Head of FIU-NL was part of the team tasked with setting up the Egmont Centre of FIU Excellence and Leadership (ECOFEL).

547. Co-operation between FIU-NL and other European FIUs is a strength. For example, FIU-NL is active in EU co-operation initiatives such as the Europol Financial Intelligence Public Private Partnership, and the EU FIU platform. The FIU-NL also provides information to members of the Egmont Group of FIUs. On average the FIU-NL receives approximately between 550-600 information requests per year from Egmont members. Many of these requests come from European FIUs and FIU-NL is generally able to respond to these requests within a few days, although there have been exceptional cases where requests have taken several months. Since 2020, FIU-NL has further improved the process of handling requests and incoming requests are processed immediately. Depending on the request, FIU-NL starts an in-depth analysis and/or will ask for additional information from obliged entities. This additional analysis takes up to a maximum of 30 days. In the exceptional cases the request cannot be met within the 30 day period, FIU-NL contacts the concerning FIU to inform them.

Table 8.10. Number of incoming foreign FIU requests

Year	No. of incoming requests	No. of foreign FIUs involved
2021*	603	79
2020	650	77
2019	538	80
2018	587	88
2017	692	83
2016	515	83

* Covers the period up to 18 November 2021.

548. FIU-NL works bilaterally and multilaterally with other European FIUs where a cross-border component is involved in an investigation and also shares relevant cross-border disseminations with other member states through FIU.net, which is a requirement under European regulations. Given the EU Directive's aim to compare hits and promptly identify linkages, FIU-NL shares UTRs through this platform in an automated manner. Feedback from some EU Member States note that these dissemination reports are numerous and could benefit from more context. FIU-NL provides further information and context to EU FIUs upon request. The Assessment Team considers that the Netherlands should seek a dialogue on how the quality of cross-border dissemination reports between EU FIUs can further improve so that the reports are more useful for recipient FIUs.

549. FIU-NL has partnered with FIUs in other countries on strategically important issues on several occasions. In 2019, for example, FIU-NL participated in joint analysis with Austrian and Romanian FIUs, on human trafficking and forced prostitution cases (see Box 3.7 under IO.6). During the Egmont Group Plenary in July 2019, an International Financial Intelligence Taskforce was launched under the leadership of FIU-Latvia on a sophisticated ML case. FIU-NL is one of the participating FIUs and is using this information in its own analysis.

550. Dutch LEAs have a number of channels to provide international co-operation with counterparts. The OM currently has two liaison officers in Italy and Spain and several Dutch prosecutors have been involved in EU Projects in neighbouring regions, including the Western Balkans. Part of the role of the liaison officers is to ensure requests for information can be dealt with as quickly as possible and to remove any barriers to information exchange that may exist. Furthermore, in 2016 the OM established a Bureau for International Affairs, which acts as an advisory body in order to provide coherent responses to international matters. One of its projects is to strengthen NL-UK law enforcement co-operation following the UK's withdrawal from EU AML/CFT and law enforcement mechanisms. The FIOD has an extensive set of international contacts and also works through the Police and liaison officers on specific matters. The FIOD/AMLC participates in EUROJUST and FCInet and regularly partners EUROPOL and INTERPOL on investigations and information sharing initiatives. Both the OM and FIOD/AMLC have participated in training and provided technical assistance to strengthen the capabilities of their foreign counterparts,

551. The Police, FIOD and KMar cooperate bilaterally through police-to-police networks and are involved in several international partnerships. They also have strong networks of liaison officers in a range of strategically important countries and regions. These officers are vital in supporting international criminal investigations and other projects. Both authorities also proactively participate in international fora and have desks at EUROPOL and INTERPOL, which help to facilitate timely international co-operation. LEAs are involved in several EUROPOL projects, such as European Money Mule Action and European Multidisciplinary Platform against Criminal Threats. KMar is also has a representative within the EU Agency for Law Enforcement Training and takes part in various international seminars.

552. The Netherlands also has a long history of co-operation with neighbouring countries, particularly Belgium and Luxembourg. As a result of the Benelux Police Treaty, Dutch Police have access to the police registers of Belgium and Luxembourg. The Benelux Treaty therefore provides powers to cross-border authorities to act without a MLA request for further efficiency.

553. Customs is able to cooperate with other authorities under several legal provisions, including the Naples II agreement for mutual assistance and co-operation between customs authorities. The Customs Information Centre (Douane Informatie Centrum, DIC) exchanges information with the EC and is involved in various EU projects, such as the EU Cash Controls Committee. It also has 39 bilateral agreements with a range of countries allowing for sharing and requesting information. All agreements extend to the BES Islands, but no information was provided on the extent to which they are used. Customs has access to the EU's CIS, but it is also not clear to what extent this is used.

554. The KSA has MoUs with other gambling authorities and is a member of the member of the GREF, a platform for European supervisors in the betting and gaming sector. The NOvA is a member of the International Bar Association and the Council of Bars and Law Societies of Europe and participates in its AML committee. DNB as supervisor of trust offices has contacts with other EU supervisors of TCSPs on specific cross-border cases. Other DNFBP supervisors and industry bodies focus less on international co-operation for sharing supervisory information. The BTWwft has one member of staff that focusses on maintaining contacts with international counterparts and has led several meetings with neighbouring countries, particularly Belgium and Germany, to share general knowledge and best practice. The Netherlands states that BTWwft has also had contact with neighbouring authorities on specific cases, but no case studies were provided to demonstrate effectiveness in this regard.

555. Representatives from the BES Islands state that, although they are not part of continental Netherlands, police requests are effectively dealt with by IRC Carib as it participates actively in ARIN-CARIB.

International exchange of basic and beneficial ownership information of legal persons and arrangements

556. The Netherlands shares basic and BO information on legal persons and other legal entities as well as on legal arrangements with its international counterparts. Basic information on legal persons and other legal entities is publicly available and easily accessible. There is a small fee to access this information in certain circumstances. Insofar as legal entities have registered this information in the BO register, the following BO information is publicly available: the name, month and year of birth, nationality, country of residence and nature and extent of beneficial interest held. Other BO information such as address and copy of identification documents are only available to competent authorities, such as OM, LEAs, FIU-NL and supervisory authorities, who are able to share this information, where appropriate. As noted in IO.5, at the time of the onsite visit, 27% of existing legal had populated the BO register. Non-public BO information can also feature in requests received for MLA and by the FIU-NL and LEAs via established formal arrangements (e.g., Egmont, EU tax sharing information, EUROPOL and INTERPOL requests). The Netherlands CLO has a specific MLA process for requests from third countries in order to ensure that requests are not of a political nature or likely to violate human rights.

557. The Netherlands actively seeks basic and BO information on foreign legal persons and legal arrangements. Competent authorities request basic and BO information from foreign counterparts in a number of ways. Where information is not publicly accessible, this can be requested as part of outgoing MLA through the CLO, as part of FIU-NL requests to other FIUs, or other formal mechanisms that individual competent authorities are engaged with, such as the Joint International Taskforce on Shared Intelligence and Collaboration.

558. Case studies demonstrated the exchange of basic and BO information. The Dutch authorities were unable to provide exact numbers of foreign requests for BO information to Dutch central, regional and other competent authorities.

BES Islands

559. Basic information on legal persons can be accessed publicly in the BES Islands. There are two company registers in the BES Islands (one for Bonaire and a joint register for St. Eustatius and Saba). At the time of the onsite the joint register was not operational because of a technical issue. Non-public information held by the CoC must be subpoenaed. Unlike continental Netherlands, the BES Islands do not have a publicly accessible BO register. In line with continental Netherlands, obliged entities need to register, identify and take reasonable measures to verify the identity of BOs when conducting CDD, but there is no requirement for legal persons or arrangements to hold BO information. The Dutch authorities were unable to determine whether competent authorities in the BES islands exchange basic and BO information with international counterparts.

8

Overall conclusions on IO.2

1. The Netherlands seeks and provides constructive MLA and extradition. While the Assessment Team was unable to assess the timeliness of MLA in practice, responses reported by the FATF global network note that international co-operation with the Netherlands is of high quality and no significant issues were raised about the timeliness of MLA and execution requests.
2. The Netherlands actively participates in a wide range of activities in order to exchange financial intelligence, and LEA and supervisory information. FIU-NL disseminates a significant number of cross-border dissemination reports to other EU FIUs, however, some feedback suggests that this type of report could benefit from more context.
3. The Dutch authorities have a large and continuously growing network of liaison officers who assist with timely co-operation and information exchange. These well working networks guarantee a high degree of informal co-operation especially during the intelligence phase in international/cross-border investigations, to locate appropriate channels for further information exchange and to speed up processes when time constraints are critical.
4. Although the Netherlands has initiated some JITs, there appears to be a lack of clarity when JITs or other mechanisms should be used and whether or not more JITs should be initiated to deliver effective outcomes. Furthermore, there is no legal basis for JITs to be established in the BES Islands.
5. Basic and some BO information on legal persons and other legal entities is publicly available in the Netherlands and to some extent in the BES Islands. Where this is not publicly available there are formal channels for foreign authorities to obtain this in a timely manner.
6. The Netherlands is rated as having a high level of effectiveness for IO.2.

TECHNICAL COMPLIANCE

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2011. This report is available from on the FATF webpage.

Recommendation 1 – Assessing risks and applying a risk-based approach

This is a new Recommendation, which was not assessed in the 3rd round MER.

Criterion 1.1 **–** The Netherlands has identified and assessed its ML/TF risks through two separate NRAs in 2017, and updated these assessments in 2020. The NRAs were developed by the WODC (the Research and Documentation Centre) of the Ministry of Justice and Security. The methodology was based on the ISO 31000 risk management framework. These NRAs identify, analyse and categorise the ML/TF methods and channels having the greatest potential risks, as well as the resilience of the policy instruments (laws, regulations, etc.) aimed at prevention and mitigation of ML/TF. The inputs were primarily qualitative (e.g., interviews and questionnaire responses), and also included quantitative data such as statistics, *inter alia,* from the Central Bureau of Statistics.

BES Islands: Separate NRAs were developed by the WODC for the BES Islands in 2018 and 2021. The NRAs assess the ML risks present in the Islands following the aforementioned methodology. The authorities did not identify any signs of TF threats when preparing the NRAs and therefore do not include any analysis on the TF threats and vulnerabilities in the BES Islands. The inputs into the BES NRA were primarily qualitative and predominantly based on experts' opinions and estimates as there is currently a lack of quantitative data on financial and economic crime on the BES Islands. FIU-NL information has been used in the latest version of the BES NRA.

Sectoral risk assessments: AML/CFT supervisors continuously monitor risks in sectors (see Core Issue 3.2). These sectoral risk assessments guide risk-based supervisory activities.

SNRA: The European Commission (EC) is responsible for the preparation of an SNRA, which identifies specific cross-border threats that could affect the EU's internal market (AMLD4, Art. 6). This SNRA identifies the parts of the internal market most exposed to risks, the risks per relevant sector and the most common ML typologies. The EC is required to update the SNRA every two years (AMLD, Art.4(1)).

Criterion 1.2 **–** The Ministers of Finance and Justice and Security are jointly responsible for assessing national ML and TF risks in the Netherlands (Wwft, Art.1f; Wwft BES, Art.1.14).

Criterion 1.3 – The Ministers of Finance and Justice and Security are required to jointly update and publish the results of the ML and TF NRAs at least every two years (Wwft, Art. 1f).

BES Islands: The Ministers of Finance and Justice and Security are required to *periodically* publish the results of the ML and TF NRAs (Wwft BES, Art. 1.14), which is defined in an explanatory memorandum as every two years.

Criterion 1.4 – The NRAs (including for the BES Islands) are required to be published, and are therefore available to competent authorities, SRBs, FIs and DNFBPs (Wwft, Art.1f; Wwft BES, Art. 1.14). All NRAs have been published on publicly accessible government websites in Dutch and English.

The Ministry of Finance and the Ministry of Justice and Security also present the results of risk assessments in relevant coordinating bodies, including the Obliged Entities Committee, the FEC and the Wwft Supervisors Consultations. In general, the findings of the NRAs have been disseminated to FIs, DNFBPs and NPOs through outreach and trainings. The findings of the sectoral risk assessments are incorporated into guidelines or guidance documents, which were disseminated to FIs and DNFBPs.

Criterion 1.5 – The Netherlands demonstrates that it is allocating resources and implementing measures based on the authorities' understanding of ML/TF risks, starting with its 2017 NRAs. A 2019 ML Action Plan was developed by competent authorities based on the findings of the ML NRAs and covers both continental and Caribbean Netherlands. The detailed measures aim to mitigate the ML residual risks identified in the NRAs. This plan includes the allocation of additional resources in line with the risks identified, such as extra funds to intensify the investigation of ML. Progress reports to the ML Action Plan have also identified additional risk mitigation measures, including for abuse of legal entities and trade based ML.

Concerning the risk-based allocation of resources and implementing measures for TF, CFT is a part of the Netherlands' overall CT policy and strategy. A TF Policy Statement was approved in September 2020, and outlines measures to mitigate the four greatest TF risks.

BES Islands: Based on the specific risks identified in the 2018 and 2021 NRAs, the supervision of notaries and lawyers was enhanced, and amendments were introduced, for example, to include dealers in construction materials as obliged entities.[66] To tackle the risks identified, additional resources have been made available to the KPCN and OMCarib.

Criterion 1.6 –

(a) A supervisor may grant an exemption from the obligation to identify and assess ML/TF risks if an FI or DNFBP belongs to a sector in which the specific ML and TF risks are "clear and understandable" (Wwft, Art.2b(4)). No sectors have been exempted.

Issuers of electronic money (prepaid cards that can be exchanged with multiple parties) are not required to conduct CDD, with the exception of transaction monitoring, if the balance does not exceed EUR 150, cannot be reloaded, the electronic money is used exclusively for the purchase of goods or services, and other conditions are met (Wwft, Art.7.1). The issuing organisation is required to collect sufficient data

[66] Dealers in construction materials are not covered in the FATF Standards.

to verify whether the transactions fit the profile of the user of the balance (Wwft, Art.7.2).

BES Islands: DNFBPs (except for TCSPs) are exempt from the following obligations (Wwft BES, Art. 1.13):

- Identifying and assessing its ML and TF risks;
- Having in place policies, procedures and measures to mitigate ML and TF risks identified in the NRA;
- Designate a person to be responsible for ensuring compliance with the AML/CFT obligations in the Wwft BES; and
- Implementing group-wide policies and procedures.

According to the BES NRA these are not areas of proven low risk or occasional or very limited activities and are therefore not considered risk-based.

(b) The Minister of Finance may grant an exemption from the Wwft obligations to FIs and DNFBPs who perform activities on an incidental or very limited basis, proven that there are low ML and TF risks (Wwft, Art.1c(1); Wwft BES, Art.1b(1)). No exemptions have been issued. There is currently no decree that grants such exemptions to FIs and DNFBPs in the BES Islands.

Criterion 1.7 – FIs and DNFBPs must conduct CDD in line with the identified ML and TF risks of their customers, business relationships, products or transactions (Wwft, Art.3(8); Wtt, Art. 33-36; Wwft BES, Art.1.8). At a minimum, risk sensitivity of FIs and DNFBPs (in continental Netherlands) should be based on the risk indicators listed in Annex I or III of AMLD4 (Wwft, Art. 3(9); Wtt, Art. 33(2) for trust offices). However, FIs and DNFBPs in the BES Islands must, at a minimum, take into account the risk factors designated by the Minister in a regulation (Wwft BES, Art.2.5(1)).

FIs and DNFBPs must perform enhanced CDD where higher risks are identified, such as for identified high risk countries, large transactions and transactions with unclear patterns, and for PEPs (Wwft, Art.8(4-9); Wtt, Art.33-36**)**. In the BES Islands, FIs and DNFBPs must perform enhanced CDD where higher risks are identified, including for PEPs and correspondent banking (Wwft BES, Art.2.10).

Criterion 1.8 – The Netherlands (including the BES Islands) allows simplified due diligence measures where low-risk has been identified (Wwft, Art.6; Wwft BES, Art.2.8). Simplified due diligence is not permitted when the FI or DNFBP suspects ML or TF (Wwft, Art.3(5)(c); Wwft BES, Art.2.3(c)).

Criterion 1.9 – Supervisors and SRBs are required to ensure that FIs and DNFBPs are implementing their obligations under R.1 (Wwft, Art.1d).

BES Islands: Various supervisory authorities monitor compliance of FIs and DNFBPs in the BES Islands (Decree on the Designation of Supervisory Authorities, Art. 1(b)). Deficiencies exist related to risk-based measures under R.26 and R.28.

Criterion 1.10 –

a) FIs and DNFBPs are required to document their risk assessments (Wwft, Art.2b(3); Wwft BES, Art.1.9; Wtt, Art.38(g) for most TCSPs).

b) FIs and DNFBPs must take measures to identify and assess ML and TF risks related to customers, products, services, transactions, channels of supply, and geography (Wwft, Art.2b(1)-(3), Wwft BES, Art.1.9(2); Wtt, Art.14(3) and 26 for most TCSPs).

c) Risk assessments are required to be up to date (Wwft, Art.2b(3); Wwft BES, Art. 1.9(3); Wtt. Art.14(3) for most TCSPs).

d) Risk assessments must be submitted to the supervisory authority upon request (Wwft, Art.2b(3); Wwft BES, Art. 1.9(3); Wtt, Art.18 for most TCSPs).

In the BES Islands, these requirements do not apply to casinos, real estate agents, DPMS, and legal professionals (Wwft BES, Art. 1.13).

The supervisory authority may grant dispensation from the aforementioned requirements when ML and TF risks are "clear and understandable" (Wwft, Art. 2b(4); Wwft BES, Art. 1.9(4)). No such dispensations have been granted to date.

Criterion 1.11 –

a) FIs and DNFBPs must have policies, procedures and measures in place to mitigate and effectively manage ML and TF risks identified in the most recent versions of the SNRA and NRAs (Wwft, Art. 2c; Wwft BES, Art. 1.10; Wtt, Art. 14(1-3) for some TCSPs). Such measures are subject to the approval of senior management (Wwft, Art. 2c(3); Wtt, Art. 10; Wwft BES, Art.1.10(3)). In the BES Islands, these requirements do not apply to casinos, real estate agents, DPMS, and legal professionals. Deficiencies noted in c.22.1 also apply here.

b) FIs and DNFBPs must ensure that the aforementioned risk mitigation measures, policies and procedures are systematically reviewed and, where appropriate, adjusted (Wwft, Art. 2c(4); Wwft BES, Art. 1.10(3)). In the BES Islands, these requirements do not apply to casinos, real estate agents, DPMS, and legal professionals. Deficiencies noted in c.22.1 also apply here.

c) FIs and DNFBPs must perform enhanced CDD where higher risks are identified (Wwft, Art. 8(1), Wtt, Art.33-36 for some TCSPs; Wwft BES, Art.2.10(1)).

Criterion 1.12 – The Netherlands (including the BES Islands) allows simplified due diligence measures where low risks are identified and criteria 1.9 to 1.11 are generally met (Wwft, Art.6; Wwft BES, Art.2.8). Deficiencies noted under these criteria related to BES Islands are applicable here. Simplified due diligence is not permitted when the FI or DNFBP suspects ML or TF (Wwft, Art. 3(5)(c); Wwft BES, Art. 2.3(c)).

Weighting and Conclusion

The Netherlands demonstrates persistent efforts to identify and assess its ML/TF risks. The NRAs primarily rely on qualitative inputs, which may impact the quality of the conclusions on risks. Some sectors in the BES Islands are exempted from AML/CFT requirements amid the existence of identified risks but this is considered a minor shortcoming considering the materiality of these sectors in the broader context of the Netherlands.

Recommendation 1 is rated as largely compliant.

Recommendation 2 - National Co-operation and Co-ordination

In its last MER, the Netherlands was rated largely compliant with former R.31, as some co-ordination mechanisms were not used effectively and some co-ordination bodies met infrequently.

Criterion 2.1 **–** The 2019 ML Action Plan was developed based on the findings of the ML NRAs and covers both continental and Caribbean Netherlands. The ministers of Justice and Security and Finance monitor the progress of the Action Plan and report to the parliament every six months. A TF Policy Statement was also approved in September 2020, which supplements a number of existing CT and CFT policies. As no signs of TF threats were identified, no CFT policy has been developed for the BES Islands.

Criterion 2.2 **–** The Minister of Finance and the Minister of Justice and Security share responsibility for AML policies. The Minister of Finance, the Minister of Justice and Security and the Minister of Foreign Affairs share the responsibility to coordinate CFT policies pursuant to Organisation Decrees of the Ministries of Finance, Justice and Security and Foreign affairs. These authorities are the same for the BES Islands. Various co-ordination bodies exist to facilitate co-operation amongst AML/CFT authorities to avoid duplication of efforts. For example, the Minister of Finance and the Minister of Justice and Security share responsibility for AML policies and meet regularly at a Ministerial Committee for ML. For CFT, the Ministers coordinate at the Inter-ministerial Sanctions Consultation Meeting and the Joint Counter-Terrorism Committee. See IO.1 for additional information.

Criterion 2.3 **–** The Netherlands (including the BES Islands) have a wide spectrum of AML/CFT co-ordination bodies at the policy and operational levels. Top-down co-ordination between implementing authorities takes place through structural co-operation within the FEC and AMLC. A number of operational information hubs also exist to facilitate information sharing across competent authorities [e.g., iCOV and Justis(Track)]. Multidisciplinary co-operation between government parties and with the private sector is a key characteristic of the Dutch AML/CFT system (see IO.1). Similar policy and operational co-ordination bodies exist for the BES Islands.

Criterion 2.4 **–** CPF falls under the joint responsibility of the Minister for Foreign Trade and Development Co-operation and the Minister of Foreign Affairs, with the Minister of Finance responsible for PF policy (Organisation Decree of the MFA, section 9.2). A number of public sector co-ordination bodies exist with countering PF in their mandates (e.g., the Sanctions Act Consultation Meeting). Public-private co-ordination bodies also exist to raise awareness with the private sector (see IO.1). These co-ordination and co-operation mechanisms cover the BES Islands.

Criterion 2.5 **–** The Netherlands coordinates to ensure the compatibility of its AML/CFT requirements with Data Protection and Privacy rules through the European General Data Protection Regulation (GDPR), its implementation act and through the implementation of EU Directive 2016/680 (Wpg and Wjsg). All draft legislation affecting the use of personal data must be submitted to Netherlands' designated Data Protection Authority (GDPR, Art.36(4)). Before the introduction of processes that involve personal data, a Data Protection Impact Assessment must be conducted (GDPR, Art. 35).

BES Islands: The BES Personal Data Protection Supervision Commission is responsible for supervising the processing of personal data (Wbp BES, Art.49). Changes in AML/CFT legislation are consulted with the Commission.

Weighting and Conclusion

All criteria are met.

Recommendation 2 is rated as compliant.

Recommendation 3 - Money laundering offence

In its last MER, the Netherlands was rated largely compliant with former R.1 and 2. Outstanding deficiencies related to effectiveness, particularly incomplete statistics and the lack of information on types of predicate offences. Due to the lack statistics, assessors could not establish whether sanctions were fully effective.

Criterion 3.1 **–** The Netherlands (including the BES Islands) criminalises ML in line with the requirements of the Vienna and Palermo Conventions (WvSr, Art. 420bis, 420ter, 420quater; WvSr BES Art. 435a, 435b, 435c). It criminalises the concealment or disguise of the true nature, source, location, the disposition or movement of an object, or the concealment or disguise of the person who has title to or possession of the object, or the possession, acquisition, transfer, conversion and use of an object which derives directly or indirectly from any offence (WvSr, Art 420bis; WvSr BES, Art. 435a).

The *mens rea* element under the Conventions is satisfied by requiring that the offender either knows (WvSr, Art. 420bis; WvSr BES, Art. 435a) or may reasonably suspect (WvSr, Art. 420quater; WvSr BES, Art. 435c) that the object directly or indirectly is the proceeds of any offence.

The Netherlands (including the BES Islands) criminalises the habitual commission of the ML offence as a form of aggravated offence, corresponding to a higher sanction (WvSr, Art. 420ter; WvSr BES, Art. 435c).

The term "object" is defined as "all tangible property and all property rights" (WvSr, Art. 420bis; WvSr BES, Art. 435a2). Tangible properties are movable (e.g., cash, cars) and unmovable goods (e.g., real estate). Property rights are rights that are transferable or which intend to give its proprietor material benefit (BW, Art. 3:6, BW BES, Art. 3:6). The Netherlands provided case law demonstrating that this definition encompasses VAs.

Criterion 3.2 **–** Any offence (with the exception of misdemeanours) is a predicate offence to ML (WvSr Art. 420bis, 420quater; WvSr BES Art. 435a, 435c). This encompasses the full range of offences in the 21 categories of designated predicate offences and more.

Criterion 3.3 **–** The Criminal Codes distinguish between offences and misdemeanours (i.e., minor offences).The Netherlands and BES apply a threshold approach whereby all offences in the Criminal Code are predicate offences to ML.

Criterion 3.4 **–** The ML offences extend to any "object" deriving directly or indirectly from any offence, regardless of the value (WvSr Art. 420bis, 420quater; WvSr BES, Art. 435a, 435c).

Criterion 3.5 **–** It is not necessary that a person is convicted of a predicate offence to prove that property is the proceeds of crime (WvSr Art. 420bis, 420quater; WvSr BES Art. 435a, 435c). ML is an autonomous offence and merely requires the OM to establish that objects are likely to be directly or indirectly proceeds of any offence. This does not require proving that an item of value originated from a specifically indicated offence (WvSr Art. 420bis). This interpretation is applicable also to BES provisions.

Criterion 3.6 – The ML offence does not explicitly refer to the laundering of proceeds generated by a foreign predicate. However, as the laundering refers to an object deriving directly or indirectly "from any offence", there is no limitation as to the domestic or foreign origin of the predicate offence. The Supreme Court confirmed this approach: ML provisions are, at a minimum, applicable to predicate offences that have been committed abroad if the relevant conduct has been criminalised both under Dutch law and the law of the country in which it took place (ECLI:NL:HR:1998:ZD1388 ruling of 1998).

Criterion 3.7 – Self-laundering is criminalised separately from the predicate offense. However, Netherlands applies a different approach in relation to the sanctions depending on the actions that would constitute the ML offense. If the actions consist in concealing, hiding, transferring the proceeds of its own crime, although there are no explicit legal provisions, according to Dutch authorities, the conduct will fall under the ordinary definition of ML offense (WvSr, Art. 420bis; 420quater) and the person can be convicted to a term of imprisonment up to three or six years and a fine of the fifth category. Dutch case law supports this interpretation. If the action involves the mere acquisition or possession, the conduct falls under the definition of WvSr, Art. 420bis1; Art. 420quarter1, and the person can be convicted to a term of imprisonment up to six or three months and a fine of the fourth category.

BES Islands: There are no legal provisions (or case law) precluding the conviction of the perpetrator of a predicate offense for acts of self-laundering (WvSr BES, Art. 435a, 435c).

Criterion 3.8 – It is possible to infer the intent and knowledge required to prove a ML offence from the conduct itself and from objective factual circumstances. This was demonstrated through case law and applicable to the BES Islands.

Criterion 3.9 – The criminal penalty for ordinary ML is imprisonment up to six years or a fine of the fifth category (EUR 87 000) (WvSr, Art. 420bis). Habitual ML or ML committed while exercising a profession or business is punished with imprisonment not exceeding eight years, or a fine of the fifth category (EUR 87.000) (WvSr, Art. 420ter). Culpable ML (i.e., where the person had reasonable cause to suspect the illegal origin of the objects) is subject to lower sentencing: up to two years imprisonment or a fine of the fifth category (WvSr, Art. 420quater). Community sentence up to 240 hours can also be applied for all ML offences (WvSr, Art. 9). The different penalties (fine and imprisonment) can be imposed cumulatively (WvSr, Art. 9.3).

The simplified deliberate or culpable acquisition or possession of an object deriving directly from serious offences committed by the offender, where no acts have been conducted to conceal or disguise the criminal origin, is punishable with a term of imprisonment not exceeding six or three months or a fine of the fourth category (WvSr Art. 420bis1; WvSr, Art. 420quater1). The Assessment Team considers that these penalties are not proportionate or dissuasive.

With the exception of the sentences provide in WvSr Art. 420bis1 and WvSr Art. 420 quarter1, the maximum sentences for ML offence appear dissuasive and proportionate to Dutch standards when compared to the sentences for other criminal offences, such as fraud and tax offences (six years' imprisonment or a fine of the fifth

Technical compliance

category), embezzlement (three years' imprisonment or a fine of the fifth category), but significantly lower than in BES Islands.

BES Islands: The criminal penalty for ordinary ML is imprisonment up to twelve years or a fine of the fifth category [USD 56 000 (approx. EUR 45 500)] (WvSr BES, Art. 435a). Habitual ML is punished with imprisonment not exceeding sixteen years, or a fine of the fifth category (WvSr BES, Art. 435c). Culpable ML is subject to lower sentencing: up to four years' imprisonment or a fine of the fourth category [USD 14 000 (approx. EUR 11 385)] (WvSr BES, Art. 435c). The Court can impose both fines and custodial sentences, in combination with each other or apart (WvSr BES, Art. 17a(2)). The available sanctions for ML offences in the BES Islands are proportionate and dissuasive.

Criterion 3.10 **–** Legal persons can be subject to criminal liability in the Netherlands (including the BES Islands). The liability of the legal persons is not dependent on the prosecution or conviction of a natural person and does not preclude parallel criminal proceedings against the natural persons holding control (WvSr, Art. 51; WvSr BES, Art. 53). While civil and administrative proceedings are also possible, it is not possible to apply both criminal and administrative penalties for the same behaviour of the same legal person (una via principle, Awb, Art. 5:44). An administrative authority will refrain to impose an administrative fine if criminal proceedings have been instituted against the same person for the same conduct. This may impact the dissuasiveness of sanctions available for legal persons.

Administrative sanctions imposed on a legal person do not affect the validity of criminal proceedings against the involved natural person, even when this natural person had been held liable for paying the administrative sanctions imposed to the legal person (ECLI:NL:HR:2021:219).

Sanctions available for legal persons are proportionate. If the fine category specified for the offence does not provide for an appropriate punishment, legal persons may be subject to a higher fine up to the maximum of the next fine category. ML is therefore punishable with a fine of the sixth category (EUR 870 000). If more than one act or crime is committed, fines can cumulate (WvSr, Art. 57, 58). If a fine of the sixth category may be imposed for an offence and that fine category does not provide for an appropriate punishment, a fine of up to 10% of the annual turnover of the legal person in the financial year preceding the judgment or punishment order may be imposed (WvSr, Art. 23(7); WvSr BES, Art. 27(7)).

Criterion 3.11 **–** The Netherlands (including the BES islands) criminalises ancillary offences to ML through general provisions related to attempting, facilitating, assisting, soliciting or inciting, aiding and abetting, and participating in an organisation to commit offences (WvSr, Art. 45, 47, 48 and 140; WvSr BES Art. 47, 49, 50 and 146).

Weighting and Conclusion

The legal framework broadly covers the requirements of R.3 with minor shortcomings related to the available sanctions for self-laundering and the inability to apply both criminal and civil/administrative sanctions to legal persons.

Recommendation 3 is rated largely compliant.

Recommendation 4 - Confiscation and provisional measures

In its last MER, the Netherlands was rated largely compliant with the requirements of former R.3, as the scope of the legal privilege hindered appropriate access to information and documents held by lawyers and other legal professionals. Furthermore, the absence of more comprehensive statistics did not allow to conclude that confiscation measures were applied in a fully effective manner.

Criterion 4.1 **–** The Netherlands can confiscate, upon conviction, proceeds and instrumentalities of crime held by the offender and third parties (WvSr, Art. 33a and 36e; WvSr BES, Art. 35 and 38e). A confiscation order may be issued upon conviction of any criminal offence (WvSr, Art. 33 and 36e; WvSr BES, Art. 35). Confiscation provisions are therefore applicable to ML, predicate offences and TF:

- **a)** *Property laundered*: The objects in relation to which the offence was committed are liable to confiscation (WvSr, Art. 33a; WvSr BES, Art. 35);
- **b)** *Proceeds, including income or other benefits derived from proceeds, and instrumentalities used in or intended for use in ML or predicate offences*: confiscation extends to objects used, or intended for use, or manufactured for the commission of any offence, including ML and predicate offences. Confiscation extends to objects or benefits obtained from the proceeds of crime (WvSr, Art. 33, 33a and 36e; WvSr BES, Art. 35, 38e);
- **c)** *Property that is the proceeds of, used in, or intended or allocated for use in the financing of terrorism, terrorist acts, or terrorist organisations*: The same provisions apply to proceeds related to the financing of terrorism, a terrorist act or a terrorist organisation (WvSr, Art. 33; WvSr BES, Art. 35).
- **d)** *Property of corresponding value*: The Netherlands has a value confiscation regime that allows for the determination of the value of property laundered and proceeds from any criminal offense and the confiscation of the equivalent value. Confiscation also extends to proceeds from other criminal offences where there are sufficient indicators that the offender committed them or received profits from crimes, regardless of who committed them (WvSr, Art. 36e; WvSr BES, Art. 38e).

In continental Netherlands, objects are defined as property of any description, whether corporeal or incorporeal (WvSr, Art. 33a(4)), whereas the definition in the BES Islands refers to "all tangible property and all property rights" WvSr BES, Art. 35). Both definitions refer to "all tangible property and all property rights", which covers property of any description, whether corporeal or incorporeal.

Proceeds held by third parties can be seized and confiscated if they knew or could have reasonably suspected that the property was derived from a criminal act (object confiscation, WvSr, Art. 33a (2); WvSr BES, Art. 35 (2)), as well as if they came in the possession of a third party with the apparent intention of impeding or preventing seizure, (WvSv Art. 94a (4 and 5) and WvSr, Art. 36e).

Criterion 4.2–

- **a)** *Identification, tracing and evaluation*: Financial investigations are initiated in all criminal investigations where suspicious flows of money or assets are identified (Confiscation instruction 2016A009, Chapter 4). For offences, punishable with a fifth category fine, a criminal financial investigation (SFO) may be initiated independently of the investigation into the predicate offences

(WvSv Art.126 and WvSv BES, Art. 177a). In these cases, investigating officers can obtain data or documents held by any person except the suspect, without any further authorisation (WvSv, 126a). In a general criminal investigation (including financial investigation), upon authorisation from the OM, investigative officers can obtain data held by any person, including FIs and DNFBPs (WvSv, Art. 126nc and 126nd; WvSv BES, Art. 177b). Furthermore, an investigation into the assets of a convicted person may be initiated, where necessary for value confiscation (WvSv, Art. 6:4:11(2)).

b) *Provisional measures*: Property subject to confiscation, and property that could demonstrate unlawfully obtained gains can be seized (WvSv, Art. 94; WvSv BES, Art. 119).

For the investigation of offences punishable with a fifth or forth category fine, including ML offences, property can also be seized for victim compensation and for any value confiscation/payment that may be imposed upon conviction. This prejudgement seizure is not limited to proceeds of the offense (WvSv, Art. 94a). In BES Islands, a provisional seizure can be granted for serious offences punishable with a minimum of four years of imprisonment, or offences which may result in a sizeable amount of gain (WvSv BES, Art. 119a).

Seizing measures can be issued *ex parte* (WvSv, Art. 94(3) and 103; WvSv BES, Art. 129a).

c) *Preventing or voiding actions*: In addition to the prejudgement seizure, assets belonging to a third party can be seized if there are indications that the objects, or part of them, came into the possession of the third party with the apparent intention of impeding or preventing seizure (WvSv, Art. 94a.4-5; WvSv BES, Art. 119a). The OM may declare null or fraudulent any legal act, which an accused or convicted person has entered into within one year prior to the commencement of the criminal investigation (WvSv, Art. 94d(2); WvSv BES, Art. 119d(2)).

d) *Appropriate investigative measures:* LEAs can use all the appropriate investigative measures provided in the WvSv and WvSv BES in the course of a criminal investigation of ML, TF and predicate offenses. Investigative powers for seizure of goods and assets are available during criminal investigations. These may be applied during a parallel criminal investigation into financial elements, for the purposes of confiscation (see R.31).

Criterion 4.3 – The rights of bona fide third parties are protected. Seizure based on WvSv art. 94 and object confiscation based on WvSr art. 33a regarding assets held by third parties is only possible if they had knowledge, or could have reasonably suspected that property represented proceeds or instrumentalities of crime (WvSr, Art. 33a(2) and (3) and WvSr BES, Art. 35(2) and (3)). Prejudgement seizure on third party's assets (WvSv, Art. 94a. 4 or 5) is only permitted when the third party has knowledge, or could have reasonably suspected that assets came into the third party's possession with the apparent intention of impeding or preventing seizure. Any affected person (including bona fide third parties) may challenge a seizing measure (WvSv, Art. 552a and 552b), and this decision can be appealed. This also includes filing a civil complaint against a convicted person (WvSv, Art.5:5:12, 6:6:26; WvSv BES, Art. 150, 151). The OM has the competence to authorise the sale or destruction of seized objects (WvSv, Art. 117).

Criterion 4.4 **–** Within the OM, the LBA is responsible for coordinating and managing prejudgement seized property. A specific LBA department—the AMO—manages international and foreign assets. The OM decides whether to return, retain, sell or destroy goods seized or confiscated, in consultation with asset managers working at the LBA/AMO. A department within the Ministry of Finance is the statutory depositary and manager of seized goods (Organizational Regulations for the OM 2012, Art. 2; State Movable Goods Material Management Regulations).

BES Islands: OM BES decides on the disposal of frozen, seized or confiscated objects (WvSv BES, Art. 142). The Registrar of the Court of First Instance of BES is the designated custodian of seized objects (Bbiv BES, Art. 2.1). Seized objects are managed by the custodian at the registry of the court (Bbiv BES, Art. 2.2) as per decision of the OM BES (Bbiv BES Art. 13-17).

Weighting and Conclusion

All criteria are met.

Recommendation 4 is rated compliant.

Recommendation 5 - Terrorist financing offence

In its last MER, the Netherlands was rated partially compliant with former SR.II, as the collection of funds was criminalised only if the perpetrator had acquired or possessed them; partial criminalisation of the financing of the offenses set forth the Annex to the TF Convention; limited criminalisation of the financing of an individual terrorist; the attempt to finance a specific terrorist act was not criminalised. The FUR concluded that the introduction of an autonomous TF offense in the Penal Code (WvSr, Art. 421) largely addressed these deficiencies, bringing the overall level of compliance to LC.

Criterion 5.1 **–** The Netherlands (including the BES Islands) implements the obligation to criminalise the financing of the annexed treaty offences as per Art. 2.1(a) of the TF Convention. The combined provisions of the Penal Code (WvSr, Art. 421, Art. 83; WvSr BES, Art. 435(e) and 84a) cover Art. 2.1(b) of the TF Convention. The TF offences refer to the provision of "means" or "information" and provision or collection of "objects". These definitions cover funds and other assets (see c.5.3).

Criterion 5.2 In the Netherlands (including BES Islands), the TF offence covers the *deliberate* collection, acquisition, possession and provision of objects which, wholly or partly, directly or indirectly, serve to offer financial support for the commission of a terrorist crime (WvSr, Art. 421; WvSr BES, Art. 435(e)). The Criminal Code lists the serious offences that must be considered as terrorist crimes, which are in line with the TF Convention (WvSr, Art. 83, WvSr BES, Art. 84a).

The TF offence does not explicitly cover the *mens rea* elements of "intent" and "knowledge" on the use of funds. However, the authorities explained that the use of the term "deliberate" covers the intent element under Art. 2 of the TF Convention. The "knowledge" element is considered in Dutch criminal law as a more general expression of the offender's intention. The so-called "conditional intent" requires that the offender knowingly accepts the significant likelihood that their actions will result in financial support for terrorist acts (Explanatory Memo on the introduction of WvSr, Art. 421).

While the TF offence does not refer to the financing of a terrorist organisation or an individual terrorist, the Netherlands provided case law demonstrating convictions of TF for the provision of support to an individual terrorist. However, the requirement of conditional intent implies that there is a need to establish an intentional link to the commission (or preparation) of a terrorist act. This is not sufficient to cover the financing of an individual terrorist *for any purpose*.

Furthermore, the Criminal Code criminalises the participation in an organisation which has as its purpose the commission of terrorist offences (WvSr, Art. 140a, WvSr BES, Art. 146a). The participation "shall also include the provision of financial or other material support as well as the raising of funds or the recruitment of persons on behalf of the organisation" (WvSr, Art. 140(4); WvSr BES, Art. 146a). The provision of financial or material support to a terrorist organisation is therefore broadly criminalised, regardless of whether the funds were specifically aimed at the commission of terrorist acts. However, in 2017, a judgement by the Supreme Court interpreted this provision as requiring that the financing of a terrorist organisation under Art. 140a is punishable only if the financier is a member of the organisation.

Criterion 5.2bis – In the Netherlands (including the BES Islands), there is no specific provision to cover the financing of the travel of individuals for the purpose of the perpetration, planning, preparation, participation in terrorist acts, or for providing or receiving terrorist trainings. However, the Netherlands provided case law to demonstrate that the travel to conflict zones for participating in terrorist acts or training was sanctioned as TF or as preparation of a terrorist offence (WvSr, Art. 46, 96(2)). As travelling to conflict zone was considered as either a terrorist offence or a preparation for a terrorist offence, its financing is also punishable under WvSr, Art. 421 (WvSr BES, Art. 435(e)). In the BES Islands, there are provisions to criminalise the preparation or facilitation of terrorist acts (WvSr BES, Art. 48a, 140a)).

Criterion 5.3 – The TF offence refers to the provision of "means" or "information", or the collection or provision of "objects" which serve to provide financial support. There is no limitation as to their licit or illicit origin. The Criminal Code defines "objects" as all tangible property and property rights (WvSr, Art. 420, 421; WvSr BES, Art. 435(e)). The combined use of the terms "means", "information" and "objects" covers all ways in which financial and economic support is offered to commit acts of terrorism or acts directly related thereto (Explanatory Memo, Art. 3.2). This is sufficient to encompass the funds or other assets prescribed under the FATF Standards.

Criterion 5.4 – In the Netherlands (including the BES Islands), there is no requirement that the objects were actually used to carry out or attempt a terrorist act, or be linked to a specific terrorist act. It is sufficient that the offender was aware of the significant likelihood that their acts could serve to provide support for the commission of terrorist acts.

Criterion 5.5 **–** Intent and knowledge can be inferred from objective factual circumstances, based on Supreme Court's case law (ECLI:NL:HR:2004:AP2124; ECLI:NL:HR:2005:AT4094).

Criterion 5.6 **–** In the Netherlands (including BES Islands), TF offences are punishable by a term of imprisonment not exceeding eight years or a fine of the fifth category (EUR 87 000 in the Netherlands and USD 56 000, or approx. EUR 45 500 in the BES Islands) (WvSr, Art. 421; WvSr BES, Art. 435(e)). The available sanctions for the financing of a terrorist organisation are much higher: a maximum term of imprisonment of fifteen years or a fine of the fifth category (WvSv, Art. 140a). In BES

Islands, the maximum available penalty for the financing of a terrorist organisation is a term of imprisonment of eighteen years (WvSv BES, Art. 146a). Moreover, in the Netherlands for both offences, community service up to 240 hours can be imposed (WvSr, Art. 9).

While fines and imprisonment penalties can cumulate (WvSr, Art. 9(3)), by using the conjunction "or", the provisions of the WvSr and WvSr BES explicitly admit the possibility to impose only a fine for a TF offence. This affects the dissuasiveness of the sanctions. If more than one act or crime is committed, fines can cumulate and the maximum prison sentence can be increased by one third (WvSr, Art. 57, 58). These sanctions (and in particular the possibility to apply only a fine) are not dissuasive.

Criterion 5.7 – Legal persons can be subject to criminal liability (see c.3.10). If a crime is committed by a legal person, a penalty up to the sixth category (EUR 870 000) or up to 10% of the annual turnover is possible. The liability of the legal persons is not dependent on the prosecution or conviction of a natural person and does not preclude parallel criminal proceedings against the natural persons holding control (WvSr, Art. 51; WvSr BES, Art. 53). While civil and administrative proceedings are also possible, it is not possible to apply both criminal and administrative penalties for the same behaviour of the same legal person (una via principle, Awb, Art. 5:44) (see c.3.10). This may impact the dissuasiveness of sanctions available for legal persons.

Criterion 5.8 – The Netherlands (including the BES Islands) has ancillary offences applicable in all crimes under the Criminal Code, including TF. This includes attempting to commit an offence, participating as an accomplice, organising or directing others and contributing to the commission of an offence by a group of persons acting with a common purpose (WvSr, Art. 45, 48, 47, 140; WvSr BES, Art. 47, 50, 49, and 146)

Criterion 5.9 – In the Netherlands (including BES Islands), TF offence is a predicate offence to ML (see R.3).

Criterion 5.10 – The TF offence applies regardless of whether the person alleged to have committed the offence(s) is in the same country or in a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur (WvSv, Art. 421; WvSv BES, Art. 435(e)).

Weighting and Conclusion

The Netherlands is generally compliant with R.5 with minor gaps in relation to the scope of TF offences and the proportionality and dissuasiveness of sanctions.

Recommendation 5 is rated largely compliant.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its last MER, the Netherlands was rated largely compliant with former SR.III. Outstanding deficiencies included insufficient guidance on freezing obligations other than FIs, insufficient supervision on TFS in FIs other than banks, the freezing obligations under EU Regulation 881/2001 did not expressly extend to funds and assets owned or controlled "indirectly", and the freezing was not without delay in all instances.

Technical compliance

The Netherlands implements TF TFS through EU decisions and regulations, complemented by domestic legislation. Both domestic legislation and EU legal on TFS is applicable to the BES Islands (Sw, Art. 14 et seq.; Sanction Regulation BES, Art. 1).

Criterion 6.1 **–** In relation to designations pursuant to the UNSCRs 1267/1989/2253 and 1988:

a) The MFA is the competent authority for proposing persons or entities for designation to the UN Sanctions Committees (including the BES Islands) (Sw, Art. 1c and 2, Sanction Regulations BES; BVO Protocol, Art. 1.1.3). It acts in agreement with the Ministers of Finance and of Economic Affairs, Agriculture and Innovation for designations pursuant to the 1988 Committee, and in consultation with the Ministers of Finance and Justice for designations to the 1267/1989 Committee.

b) The BVO Protocol describes the mechanism for identifying targets for designation. When the MFA is notified by the authorities of an individual/entity suspected to be involved in terrorist activities, it convenes the Asset Freezing Committee. The Committee includes representatives from the MFA, Finance, Justice and Security, OM, the FIU-NL and AIVD. After consulting with the Committee, the MFA can recommend the listing of a person to the UN 1267 Committee, regardless of whether the individual has been listed domestically. The authorities explained that the same process would apply to 1988 designations; however, there is no reference to UNSCR 1988 in the BVO Protocol.

c) The BVO Protocol does not mention the evidentiary standard of proof set out in UNSCRs 1267, 1989, 1988 and their successor resolutions for designation proposals. The listing criteria are set out in the UNSCRs and corresponding EU decision (2011/486) and regulation (753/2011). However, the EU decision and regulation do not include information on the process for member states to identify targets for designation based on UNSCR criteria.

d) The Netherlands authorities indicated that the MFA uses the approved procedures and forms for the listing of individuals, groups or entities prescribed by the relevant sanctions committee to propose a listing. However, as no designation proposal has been made so far, there is no documentary evidence available.

e) The MFA will make available to the 1267 Committee information supporting the decision to place the person or entity on the UN list (BVO Protocol, Para. 3.2.2). This information must be sufficiently specific, and its source must be indicated if possible. The status of the Netherlands as a designating state is made known to the Committee.

Criterion 6.2 **–** As an EU Member State, the Netherlands (including BES Islands) implements the requirements of UNSCR 1373 through EU and national measures.

a) *At national level*, the MFA is responsible for domestic designations, in consultation with the Minister of Finance and the Minister of Justice and Security (Anti-Terrorism Sanctions Order 2007-II, Art. 2), including for designations at the request of another country.

At the EU level, the Council is responsible for designating persons or entities that meet the criteria set forth in UNSCR 1373 (EU Regulation (CR) 2580/2001, Art. 2(3); CP 2001/931/CFSP, Art. 1(4)). The Council can also designate persons, groups and undertakings associated with ISIL and Al-Qaida or related cells or groups (CD 2016/1693/CFSP).

b) *At national level,* the MFA is notified by either the AIVD or OM if persons or entities are suspected of involvement in terrorist activities. The MFA convenes the Asset Freezing Committee and, if there are sufficient indications that the persons or entities meet the criteria for designation in UNSCR 1373 (BVO Protocol, Art. 2.1), decides on the designation, which is presented for approval to the Minister of Foreign Affairs, the Minister of Finance and the Minister of Justice and Security (see c. 6.1(b)).

At EU level, proposals for listing can be submitted by Member States' competent authorities (the MFA for the Netherlands) as well as by the High Representative for Foreign Affairs and Security Policy (CP 2001/931/CFSP, Art. 1(4); CD 2016/1693/CFSP, Art. 5)).

The Council Working Party on restrictive measures to combat terrorism (COMET WP) prepares and makes recommendations for designations. This includes assessing whether the information available meets the specific criteria for designation under UNSCR 1373 (CP 2001/931/CFSP, Art. 1(2) and CR 2580/2001, Art. 2(3)).

c) *At national level,* the MFA determines whether the third country request is supported by reasonable grounds to believe that the proposed designee meets the UNSCR 1373 designation criteria (BVO Protocol, Art. 2.4). The BVO convenes on a regular basis or ad-hoc basis in urgent cases. The time to process requests from third countries depends on the time needed by the OM and AIVD to compare the information received with their own information.

At the EU level, the EEAS or relevant Member State will carry out a preliminary scrutiny of the proposal and gather relevant information, including additional information from the requesting country (doc. 14612/1/16 REV 1 on establishment of COMET WP, Annex II, Art. 3). Delegations have 15 calendar days to review the proposal(s) and to forward the information to competent national authorities. Exceptionally, the EEAS or a delegation may put forward a request to shorten this deadline (doc. 14612/1/16 REV 1 on establishment of COMET WP, Annex II, Art.8-9).

d) *At national level,* the evidentiary standard of proof for domestic designations pursuant to UNSCR 1373 refers to "sufficient indications" that the person belongs to the category of persons and entities referred to in UNSCR 1373, and it is not conditional upon the existence of a criminal proceeding (BVO Protocol, Art. 2.1).

At the EU level, the Council decides on the basis of precise information or material supporting the decision taken by a competent authority, based on serious and credible evidence or clues, or condemnation (CP 2001/931/CFSP, Art. 1(4)). The proposals for designations are not conditional upon the existence of a criminal proceeding.

e) In the Netherlands, there are no formalised procedures to request another country to give effect to the actions initiated under the freezing mechanism. The Netherlands indicated that the same procedure as the one for requesting the EU to give effect to an asset-freezing measure at the recommendation of the Netherlands would apply and that the designation proposal would be communicated through Diplomatic Note Verbale. However, no supporting document was provided as there has been no request to a third country in recent years. At the European level, there is an alignment procedure that allows for requesting non-EU member countries to give effect to the EU list.

Criterion 6.3 –

a) At national level, the AIVD, OM and other LEAs have the powers to collect and solicit information to identify persons or entities (Wiv 2017, Art. 25 et seq.; RO, Art. 124 Book 2; WvSv, Art. 126nc et seq.).

At the EU level, all Member States shall provide each other with the widest possible range of police and judicial assistance in matters related to persons/entities that meet the criteria for designation, inform each other of any measures taken, and cooperate and supply information to the relevant UN Sanctions Committee (CP 2001/931/CFSP, Art. 4; CR 2580/2001, Art. 8; CR 881/2002, Art. 8).

b) While there is no explicit provision in sanction-related legislation to operate *ex* parte, the General Administrative Law Act envisages the possibility to operate without prior notification if the purpose of the administrative decision can be achieved only if the interested party is not informed of it beforehand (Awb, Art. 4.11(c)). The BVO Protocol explains that the measure must be in place before the persons or entities concerned are alerted (BVO Protocol, Art. 1.1.3). The publication of the freezing measure in the Government Gazette and notification of the designated persons or entities happens after the freezing measure is taken (BVO Protocol, Art. 2.5). *At the EU level*, designations take place without prior notice (CR 1286/2009, Preamble, para. 5).

Criterion 6.4 **–** The implementation of TFS pursuant to UNSCRs 1267/1989/2253 and 1988 occurs without delay. To overcome the delays in the transposition of designations at the EU level, the UN designations are in force in the Netherlands from the date of their publication by the UN and until the EU provisions enter into force (Implementation (Bridging) Sanctions Order 2019, Art. 2). In relation to TFS pursuant to UNSCR 1373, the decision to freeze funds takes effect on the day of publication in the Government Gazette and must be implemented immediately (Anti-Terrorist Sanctions Order 2007-II, Art. 2)

Criterion 6.5 **–** In the Netherlands (including BES Islands), the following provisions are in place to ensure the implementation and enforcement of TFS:

a) Under the EU regulations, all natural and legal persons within EU member states shall freeze without prior notice and delay the funds or other assets of designated persons and entities (CR 753/2011, Art. 3 and 14; CR 881/2002, Art. 2(1) and 11; CR 2580/2001, Art. 2(1a) and 10). The Netherlands also applies these freezing measures to EU residents (Anti-Terrorism Sanction Order 2002-II, Art. 1). The same obligation applies to everyone present in the Netherlands, all Dutch natural and legal persons and all Dutch nationals outside of the Netherlands (Sw, Art. 13, WED, Art. 1(2) and WvSr, Art. 2).

b) *At the EU level,* freezing actions for UNSCR 1267/1989/2253 and 1988 apply to all funds and economic resources belonging to, owned, held or controlled directly or indirectly by the designated person or entity or a third party acting on their behalf or at their direction (CR 753/2011, Art. 3; CR 881/2002, Art.

2(1)). This extends to interest, dividends, or other income or value accruing from or generated by assets (CR 881/2002, art. 1.1; CR 753/2011, art. 1(a)). There is no explicit reference to assets jointly owned, although this is covered in non-binding EU Best practices for the implementation of restrictive measures (para. 34) and EU Council Sanctions Guidelines (para. 55a).

For EU designations as per UNSCR 1373, the freezing obligation applies to all funds, other financial assets and economic resources belonging to, or owned or held by the designated person or entity (EU Regulation 2580/2001, Art. 2.1(a)). There is no explicit reference to the freezing of funds or other assets controlled by, or indirectly owned by, or derived from assets owned by, or owned by a person acting on behalf of, or at the direction of a designated person or entity. However, this gap is largely addressed as the European Council is empowered to designate any legal person or entity controlled by, or any natural or legal person acting on behalf of, a designated person or entity (EU Regulation 2580/2001, Art.2(3) (iii) and (iv)).

At national level, the Anti-Terrorist Sanctions Orders 2007 and 2007-II implementing UNSCR 1373 apply to "all assets belonging to" the designated person or entity (Art. 2). The Guidance paper on TFS by the Ministry of Finance and the DNB Guidance on Wwft and SA clarify that this includes assets derived or generated from funds or jointly owned assets. The Guidance also refers to the application of freezing measures whenever a relationship with a designated person or entity is established, and that this should be interpreted as broadly as possible. However, this guidance is not legally enforceable.

c) *At national level*, it is forbidden to directly or indirectly make assets available to designated persons or entities or to provide financial services to them (Anti-Terrorist Sanctions Orders 2007 and 2007-II, Art. 2). The non-binding Guidance papers by Ministry of Finance Guidance on TFS and the DNB guidance on the Wwft and SA explain that this must be applied very broadly.

At the EU level, for UNSCR 1267/1989 and 1988, there is a prohibition for all natural and legal persons to make funds or other resources available, directly or indirectly, to or for the benefit of designated persons or entities (CR 753/2011, Art. 3(2) and 14; CR 881/2002, Art. 2(2) and 11). However, there is no reference to entities owned or controlled, directly or indirectly, by designated persons or entities, nor to persons or entities acting on behalf, or at the direction of, designated persons or entities. The same prohibition applies for UNSCR 1373 designations; however, this gap is largely mitigated by the European Council power to designate any legal person or entity controlled by, or any natural or legal person acting on behalf of a designated person or entity (EU Regulation 2580/2001, Art. 2(3) (iii) and (iv)).

The non-binding EU Guidelines and Best Practices on TFS implementation clarify that these provisions shall be interpreted very broadly.

d) *At national level*, designations are published in the Government Gazette and a consolidated sanction list is published on the government website. There is an additional notification system in place available only to those FIs and DNFBPs who have subscribed, transmitting notifications immediately after any modification to the national list. DNB informs subscribers of national and international sanction lists through monthly newsletters. Subscription is open to anyone through the DNB website. As the newsletter is issued monthly, the changes to the list may not be communicated immediately. DNB transmits ad hoc newsletters when new national listings are adopted, but this notification may also occur with a delay. Several authorities provide guidance on the implementation of TFS, through information available on their webpages as well as guidance papers, newsletters, circulars and other policy statements.

Designations made pursuant to EU regulations are published in the Official Journal of the EU. A consolidated sanction list is available on the EC website and updated after any change to the list. However, there is a delay of a few days between the UN designations and the publication by the EU. Guidance on the implementation of the EU sanctions is available on the websites of the EC, the European Council and the European External Action Service.

e) *At national level*, the obligation to immediately report positive matches (i.e., identified relationships with a designated entity/person) only applies to FIs and TCSPs (Sw (Supervision), Art. 3). For other DNFBPs, there is no reporting obligation. In the BES Islands, VASPs and all DNFBPs except TCSPs have no obligation to report matches (Wwft BES, Art. 3:13).

At the EU level, FIs and DNFBPs are required to report any assets frozen or actions taken in relation to designed persons or entities (CR 2016/1686, Art.10; CR 881/2002, Art. 5; CR 753/2011, Art. 5; EU Regulation 2580/2001, Art. 4).

f) *At the EU level*, there are measures in place to protect the rights of bona fide third parties when implementing the obligations under R.6 (EU Regulation 881/2002, Art. 6; EU Regulation 753/2011, Art. 7). However, there are no similar legal measures at national level.

Criterion 6.6 –

a) The MFA is responsible for submitting delisting requests to the relevant UN Sanctions Committees, if the Asset Freezing Committee considers that there are no longer grounds for an asset freeze (BVO Protocol, para. 4). The BVO Protocol and the Ministry of Finance's Guidance on TFS explain how to submit a delisting request directly to the UN 1267/1989 Sanction Committee. However, there is no information in relation to requests to the 1988 Committee.

b) *At national level*, the Netherlands has procedures in place to submit delisting requests to the Asset Freezing Committee (Ministry of Finance's Guidance on TFS, question 14; BVO Protocol, para. 4). In case of an EU listing, the MFA will submit a delisting proposal to the EU. *At the EU level*, de-listing procedures are available under Regulation 2580/2001.

c) *At national level*, a designated person can submit an objection to the MFA and, if this is denied, can contest the decision before an administrative court (Awb, Art. 6:4). It is possible to lodge an appeal against the decision of an administrative court, with the Administrative Jurisdiction Division of the Council of State (Awb, Art. 6:4 (3)).

At the EU level, designated persons and entities may institute a proceeding before the EU Court of Justice (Treaty on the Functioning of the EU, Art. 263, para. 4 and Art. 275, para. 2).

d) *At national level,* if a Dutch national or resident is designated pursuant to UNSCR 1988, the MFA would notify him and inform him about the possibility to seek delisting through the MFA or the Focal Point mechanism under UNSCR 1730. *At the EU level,* persons designated pursuant to UNSCR 1988 would be informed of applicable de-listing procedures (CR 753/2011, Art. 11; CR 881/2002, Art. 7a).

e) *At national level,* for designations pursuant to UNSCR 1267/1989, the MFA would notify the individual/entity of the possibility to seek delisting through the MFA or the UN Office of the Ombudsperson (BVO Protocol, para. 3.2.2). *At the EU level*, the same provisions mentioned under c.6.6d would apply.

f) *At national level*, persons inadvertently affected by a freezing measure can object as per the procedure explained under c.6.6c, or contact the FIs where the assets have been frozen. If an FI receives information that a match could be a false positive, it shall contact the supervisor to discuss whether the freezing can be lifted (Ministry of Finance Guidance on TFS, 1.5.5).

At the EU level, there are procedures to handle cases of mistaken identity (EU Best Practices on the implementation of restrictive measures, para. 8-17).

g) *At national and EU levels*, the same procedures in place to communicate changes to the list and provide guidance, as described under c.6.5d, apply to delisting and unfreezing.

Criterion 6.7 – At the EU and national levels, there are procedures to authorise access to frozen funds, where necessary for basic expenses or for the payment of certain fees (CR 753/2011, Art. 5; CR 881/2002, Art. 2a; EU Regulation 2580/2001, Art. 5 and 6; BVO Protocol, para.3.1.2 and 3.2.2, Sanctions Order ISIS and Al Qaida 2016, Art. 5; Sanctions Order Afghanistan 2011, Art. 2; Sanction Order 2007-II, Art. 3). The Minister of Finance is the competent authority to consider these requests.

Weighting and Conclusion

There is a mechanism in place to implement TFS pursuant to relevant UNSCRs without delay, through the national and EU frameworks. However, national legislation does not always prescribe in detail how the existing provisions shall be implemented and existing guidance only partially covers this gap. Furthermore, there is no national obligation for some DNFBPs to communicate the assets frozen or actions taken in compliance with TFS obligations. Communication of designations or de-listings to FIs and DNFBPs does not always occur immediately.

Recommendation 6 is rated largely compliant.

Recommendation 7 – Targeted financial sanctions related to proliferation

This is a new Recommendation, which was not assessed in the 3rd round.

The Netherlands implements PF TFS through EU decisions and regulations. The requirements of UNSCR 1718 are implemented through CD 2016/849 and CR 2017/1509, while UNSCR 2231 requirements are implemented through CD 2010/413 and CR 267/2012. The EU regulations have direct effect in the Netherlands. Where necessary, domestic legislation complements the EU framework, through the North Korea Sanctions Order 2017 and the Iran Sanctions Order 2012.

Both domestic legislation and EU legal acts on TFS are applicable to the BES Islands (Sw, Part 7, Art. 14 et seq.; Sanction Regulation BES, Art. 1).

Criterion 7.1 **–** UN designations are in force from the date of their publication by the UN and until the provisions of the EU enter into force (Implementation (Bridging) Sanctions Order 2019, Art. 2). This measure overcomes the transposition delays of UN designations at the EU level. This is applicable to the BES Islands.

Criterion 7.2 **–** The Netherlands (including BES Islands) has identified authorities responsible for implementing and enforcing TFS, as follows:

- **a)** The EU regulations require all natural and legal persons within the Member States to freeze the funds and other assets of designated persons and entities (EU Regulation 2017/1509, Art. 34; EU Regulation 267/2012, Art. 23 and 23a). They are directly applicable in the Netherlands. The Implementation (Bridging) Sanctions Order 2019 allows for the implementation of the freezing measure without delay (see c. 7.1).
- **b)** The freezing obligation extends to all funds and economic resources belonging to, owned, held or controlled by a designated person or entity (CR 2017/1509, Art. 34; CR 267/2002, Art. 23 and 23a). This includes funds or other assets derived or generated from such funds (CR 2017/1509, Art. 2, CR 267/2002, Art. 1). There is no explicit mention to funds or assets jointly owned. However, the non-binding EU Best practices for the implementation of restrictive measures cover cases of joint ownership (para. 34). Finally, there is no reference to funds or assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities. However, these situations are covered by the requirement to freeze funds or assets "controlled by" a designated person or entity. Furthermore, the EU regulations largely address this gap, by requiring the designation of any person or entity acting on behalf or at the direction of designated persons or entities (CR 2017/1509, Art. 34(5); CR 267/2012, Art. 23a (2)(c)). The non-binding domestic guidance by the Ministry of Finance also explains that the freezing measures shall be applied whenever a relation with a designated person or entity is identified, and that this concept shall be applied very broadly.
- **c)** There is a prohibition for all natural and legal persons within EU Member States to make funds or economic resources available, directly or indirectly, to or for the benefit of a designated person or entity (CR 2017/1509, Art. 34; CR 267/2012, Art. 23 and 23a)).
- **d)** As described under c.6.5d, all EU regulations are published in the Official Journal of the EU. The EU maintains a consolidated list of designated individuals on its website and updates it after any change to the list, of which subscribers are informed of immediately by an automated e-mail. Guidance on the implementation of EU sanctions, including on the freezing obligation, is available. *At national level,* the list is published on several government websites and there are subscriptions and newsletters to facilitate information to the private sector, but this domestic communication is not always immediate. Guidance papers are also available.
- **e)** The EU regulations require all natural and legal persons within the Members States to provide immediately any information to the EC and national competent authorities to facilitate compliance with TFS pursuant to UNSCRs 1718 and 2231 (EU Regulation 2017/1509, Art. 50; EU Regulation 267/2012, Art. 40). *At national level,* the same deficiencies noted under c.6.5e apply: in

the Netherlands, besides FIs and TCSPs, there is no obligation to report sanction matches and freezing measures to the supervisor (Sw, Art. 3). In the BES Islands, there is no obligation to report for certain categories of FIs and for all DNFBPs except TCSPs.

f) There are provisions in place to protect the rights of *bona fide* third parties when implementing the obligations under R.7 in good faith (EU Regulation 1509/2017, Art. 54; EU Regulation 267/2012, Art. 42).

Criterion 7.3 – EU regulations require Member States to take all measures to ensure that TFS are implemented, and have effective, proportionate and dissuasive sanctions available for non-compliance (EU Regulation 2017/1509, Art. 55; EU Regulation 267/2012, Art. 47). At national level, FIs and trust offices shall take administrative and internal control measures to comply with the sanction regulations. This includes control of any match between the identity of a relation and designated persons or entities, and the obligation to report immediately any positive match to their supervisor (DNB or AFM) (Sw (Supervision) Regulation, Art. 2 and 3). Failure to report is an offence punishable by a term of imprisonment of up to six years, community service or a fine of the fifth category (EUR 87 000) (WED, Art. 1(2) and Art. 6) in European Netherlands and by imprisonment up to two years or a fine of the fourth category (maximum USD 14.000) or the fifth category (USD 56 0000) for legal entities (Wwft BES, Art. 6.1 WvSr BES Art. 27) in the BES Islands. However, for most DNFBPs there is no obligation for mandatory screening systems or for reporting information to their supervisor.

Criterion 7.4 –

a) *At the EU level*, petitioners of PF TFS can submit de-listing requests either through the UNSCR 1730 Focal Point, or through their government (EU Best Practices on the implementation of restrictive measures, para. 23). *At national level*, if a Dutch national or resident is designated pursuant to UNSCRs 1718 and 2231 and approach the government for guidance, the MFA would inform the person about the legal consequences of being listed and the possibility to seek delisting through the MFA or the UNSCR 1730 Focal Point. Guidance is also provided on delisting procedures at EU and UN level (Ministry of Finance's Guidance on TFS, p. 15).

b) *At the EU level*, there are procedures in place to deal with cases of mistaken identity (EU Best Practices on the implementation of restrictive measures, para. 8-17). *At national level*, persons inadvertently affected by a freezing measures can contact the MFA through the general national government website. Any questions relating to freezing measures are forwarded to the MFA and answered within four weeks. However, this process is not explained, which raises questions as to whether affected persons would be aware of it.

c) The EU regulations authorise access to funds or other assets in line with relevant UNSCRs (CR 2017/1509, Art. 35-36; CR 267/2012, Art. 24-28). *At national level*, the Minister of Finance and the Minister for Foreign Trade and Development Co-operation are the competent authorities to assess and authorise access to funds or economic resources (Iran Sanctions Order 2012, Art. 3(3); North Korea Sanction Order 2017, Art. 5). The Ministry of Finance Guidance on TFS refers to the Ministry of Finance as the competent authority to authorise sanction exemptions (Chapter 1.8).

d) The same mechanisms described under c.7.2d apply to delisting and unfreezing communications. In cases where a reported freezing action is determined by the Ministry of Finance not to be an "exact hit", DNB or AFM will communicate this immediately to the relevant FI. However, it is unclear how this process would work for other obliged entities than those supervised by DNB and AFM.

Criterion 7.5 **–** With regard to contracts, agreements or obligations that arose prior to the date on which the account became subject to TFS:

a) The EU regulations permit to add interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date when they became subject to the provisions of this resolution, provided that these amounts are also frozen. (CR 2017/1509, Art. 34(9); CR 267/2012, Art. 29).

b) The EU regulations imposing TFS pursuant to UNSCR 2231 permit the payment of sums due under a contract entered into prior to the designation of such person or entity, provided that this payment does not contribute to an activity prohibited by the regulation, and after prior notice is given to the UN Sanctions Committee (CR 267/2012, Art. 25).

Weighting and Conclusion

Through the EU and national framework, the Netherlands (including the BES Islands) has a system in place to ensure the implementation of PF TFS without delay. However, there are some minor shortcomings in relation to the extent of the freezing obligation. There is a general obligation for all persons and obliged entities to implement PF TFS. However, most DNFBPs have no obligation to implement a screening system or report information to their supervisor. Since there are no obligations, there is also no monitoring or sanctioning available for those DNFBPs.

Recommendation 7 is rated largely compliant.

Recommendation 8 – Non-profit organisations

In its last MER, the Netherlands was rated largely compliant with the requirements of former SR.VIII. Outstanding deficiencies related to the lack of outreach initiatives for NPOs outside the Central Bureau for Fundraising (CBF) seal mechanism and the lack of co-ordination and information exchange mechanisms involving the CBF.

Criterion 8.1 **–** Dutch law does not provide for a definition of NPOs. Legal entities corresponding to the FATF definition of NPOs usually take the form of a foundation or an association. Foundations have no members and their purpose is to realise a charitable objective. An association is a partnership between two or more members to achieve a certain objective.

a) The Netherlands identify foundations and associations with charitable purposes as the subset of NPOs falling within the FATF definition. Most NPOs form a low risk of TF due to their membership of a sector organisation and related self-regulation, good governance and transparency policies. However, the 2017 and 2020 TF NRAs found the acquisition and/or financing via foundations or other legal entities as the greatest TF risk. The Netherlands used different sources of information to determine the subset of NPOs likely to be at risk of TF abuse. These included the results of the 2020 TF NRA, quarterly terrorism threat assessments by the NCTV, TF investigations involving NPOs, and public-private co-operation to compose a risk profile of NPOs that could be abused (see c.8.5a). On this basis, the authorities identified foundations with potential ties to jihadist groups as posing a higher risk of TF abuse.

b) The 2020 TF NRA and some quarterly terrorism threat assessments, which are publicly available include threats related to the potential abuse of NPOs for TF. The main categories of threats identified in various threat assessments were the abuse of NPOs operating in, or close to, areas where terrorists operate; ML, fraud or TF risks related to the financing by foreign radical groups to influence certain religious foundations in the Netherlands; abuse of foundations to collect funding (e.g., for aid projects) in the Netherlands, to finance TF in the Netherlands or abroad. The 2020 TF NRA also highlights the same threats for NPOs.

c) There has been no recent formal review focussing specifically on the adequacy of measures related to the subset of NPOs at risk of TF abuse. However, the Netherlands considers the outcomes of regular TF threats analysis to identify and address any weaknesses in the measures taken to protect NPOs from potential TF abuse. Following the threat assessments, the government took measures to increase transparency in the sector (see c.8.2a).

d) The Netherlands periodically reassesses information on the NPO sector to ensure effective implementation of measures, through the quarterly threat assessments by the NCTV, which also includes information and trends related to the sector, and through the TF NRAs.

BES Islands: c.8.1(a)-(d): The Netherlands does not identify a high TF risk on the BES Islands nor a TF risk within BES NPOs. Unless explicitly mentioned in the analysis, no specific measures or actions have been taken or apply to the BES islands. No specific subset of NPOs on the BES Islands has been identified as falling within the FATF definition.

Criterion 8.2

a) The Netherlands has policies in place to promote accountability, integrity and public confidence in the administration and management of NPOs. JustisTRACK continuously monitors the integrity of legal persons, including its directors and affiliated persons or legal persons. As it has no access to information from government organisations in the BES islands, any analysis on NPOs located in the BES Islands could only be performed based on publicly available information. There are two certification systems rewarding NPOs (including in the BES Islands) that fulfil certain requirements in terms of transparency and accountability. The Tax and Customs Administration delivers the ANBI (Public Benefit Organisation) status. The ANBI status provides certain tax exemptions, with the objective to stimulate charity. NPOs that want to raise funds can apply for a certification by the Netherlands Fundraising accreditation agency (CBF). To qualify for ANBI status or CBF recognition, NPOs have to fulfil standards regarding accountability, integrity, and transparency. In the Netherlands, 32 762 foundations and 2 723 associations have an ANBI status (see IO.10), while in the BES Islands 12 out of 717 associations and foundations have ANBI status. Only 630 organisations have a CBF recognition. Finally, the Netherlands has introduced a "validation

Technical compliance

system philanthropy", compulsory for all ANBI organisations that includes a code of conduct, a certification system and a central information portal.

b) The Netherlands has undertaken outreach programmes to raise awareness on potential vulnerabilities of NPOs to TF abuse, in co-operation with the private sector. Outreach to the donor community is carried out mainly through the ANBI and CBF certifications, which signal the accountability and integrity of NPOs. The Ministry of Finance organised a series of roundtables and public-private dialogue in co-operation with the Human Security Collective to exchange on several issues, including TF risks. Roundtables have involved Dutch association of banks (NVB), large banks, NPOs of different sizes, the DNB and the Ministries of Justice and Security, Finance and MFA and the FIU. The FIU-NL also held a presentation at the CBF on the risks of abuse on NPOs in relation to TF. The roundtables have also involved some good faith NPOs most exposed to TF threats. NPOs in the BES Islands have not been targeted specifically, due to the low risk of TF.

c) As described under c.8.2b, the authorities have worked closely with NPOs in the development of best practices to address TF risks and vulnerabilities (factsheet; roundtables). These initiatives involve NPOs vulnerable to potential TF abuse.

d) The roundtables conducted by the Ministry of Finance, Ministries of Justice and Security, MFA and the Human Security Collective promote a dialogue between NPOs and the financial sector to mitigate unintended effects of TF policies, such as de-risking, and encourage NPOs to use the official financial channels. NPOs with annual revenues of more than EUR 500 000 are required to conduct their transactions via regulated channels in order to qualify for the CBF recognition.

Criterion 8.3 The Netherlands gives a prominent role to self-regulation and government intervention is minimal and only where strictly necessary. There is no public supervisory authority for the non-profit sector, but there is screening of NPOs at different stages of their establishment.

All associations and foundations (including NPOs) must be established via a notarial deed (Bw, 2:4). This step includes an obligation for the notary to perform CDD and report any unusual activity to the FIU. Furthermore, NPOs must register with the CoC's Company Register, providing articles of the foundation, the location, directors/supervisors, BO, and authorised agents (Hrw, Art. 5, 6, 9-17). There is also an obligation to keep information in the Register complete and up-to-date (Hrw, Art. 19). The data in the Company Register is verified every three years (Hrw, Art. 41).

The JustisTRACK system by the Ministry of Justice (see c.8.2a) uses several data sources to automatically monitor the integrity of legal persons registered at the CoC. This system might identify some NPOs with a high TF risk, for example, in case persons involved in the NPOs are on a terrorist sanction list or have criminal antecedents. The certification systems for NPOs with ANBI status or CBF recognition require them to fulfil accountability, integrity and transparency criteria. Tax and Customs Administration continuously supervise organisations with ANBI status, using a risk-profile based on prior experiences and input from the FIOD. CBF NPOs are required to adhere to requirements set by an independent standard-setting commission, which depend on the size and capacity of each organisation. There is an annual review of the organisations under CBF supervision and an extensive review of each organisation every three years. However, for NPOs other than those with an ANBI status or CBF recognition, there is no obligation to maintain financial statements, record their transactions, or undertake similar measures to ensure transparency in their operations, nor there is a supervisory mechanism in place. The measures available do not appear to be risk-based and do not seem to target NPOs most vulnerable to TF abuse.

Criterion 8.4

a) Many NPOs are part of a sector organisation, which monitors compliance with their self-regulation obligations. The Tax and Customs Administration, CBF and two NPO branch organisations signed a co-operation agreement to synchronise the qualification system for ANBI-status and the CBF-recognition and ensure a more effective and efficient control. However, this monitoring is limited to the compliance with the terms of recognition and only applies to the minority of NPOs that apply for ANBI status or CBF recognition. NPOs without an ANBI-status or CBF recognition, or which are not part of any sector organisation are not subject to additional monitoring, apart from the measures mentioned in 8.3. Furthermore, there is no indication of any risk-based monitoring or supervisory action.

b) A large part of sanctioning non-compliance within branch organisations is dependent on CBF-recognition, ANBI status, or other labels. The ANBI-status, the CBF-recognition or other existing labels can be revoked when the NPO no longer meets the terms of recognition or the established code of conduct. There are sanctions for non-registration or false registration to the commercial and BO register of the CoC (see c.24.13). Legal entities whose activity is contrary to the public order can be dissolved.

BES Islands: In case of failure to transmit information (on time or correctly) to the commercial register, a maximum fine of USD 28 000 (approx. EUR 22 770) can be imposed.

Criterion 8.5

a) There are several initiatives to enhance co-operation and information sharing between authorities. In particular, the FEC has a programme on TF, to share information and insights into networks and methods of financing of individuals, including NPOs. The FEC TF Task-Force is a public-private partnership initiative between the Police, the FIU-NL, the OM, FIOD and some FIs. The FIU-NL also has a public-private information sharing "TF-platform" with the four largest banks, which discuss suspected TF cases, including on NPOs. Finally, the FEC also launched a "Rogue Foundations project", where co-operation between the largest banks, the OM, the FIU-NL, Police and the municipality of Amsterdam is used to compose a TF risk profile for NPOs.

b) The Netherlands has investigative expertise and capability to examine suspected TF cases involving NPOs. The FIU-NL, FIOD and the OM have appointed experts on TF and NPOs.

c) In the course of an investigation, investigative services can consult the data in the Company Register, which includes the administration and management of NPOs. Furthermore, they can request information provided by an NPO to the Tax Administration or the CBF, to qualify for the two certifications. Investigative services can also request NPOs' financial statements. The general provisions allowing authorities to request and access information are applicable also to obtain information from NPOs (see c.31.1).

d) As per the analysis under c.8.5a, there are appropriate mechanisms to ensure that, when there is suspicion or reasonable grounds to suspect that a particular NPO is involved in TF, this information is shared with competent authorities. When a request for information is made on the basis of the Code of Criminal Procedure, the OM must include in a timeframe in which the request must be fulfilled. In case of urgent necessity, information can also be requested verbally (WvSv, Art. 126nd(4)). LEAs can also send a LOvJ request to the FIU-NL.

Criterion 8.6 The Netherlands has identified IRCs as point of contact to respond to international requests for information regarding NPOs suspected of TF or involvement in other forms of terrorist support. The general procedures for MLA and co-operation are applicable to international requests for information on NPOs (see R.37 and 40).

Weighting and conclusion

The Netherlands has identified the subset of NPOs at higher risk of potential TF abuse, as well as ways in which those organisations can be abused. There are several outreach initiatives to raise awareness and promote accountability of NPOs, but they are not part of a clear coherent policy and have not yet reached all the NPOs most vulnerable to TF. NPOs are supervised and monitored to some extent, mainly through self-regulation mechanisms. The supervision does not always focus on the organisations most vulnerable for potential TF abuse and although many self-regulation obligations focus on the transparency of the financial situation, there are few obligations or controls related to the financial situation of other NPOs. Since the TF risk on the BES Islands is considered low, no specific NPO measures are taken. This is considered a minor deficiency due to risk and materiality.

Recommendation 8 is rated largely compliant.

Recommendation 9 – Financial institution secrecy laws

In its last MER, the Netherlands was rated compliant with the requirements of former R.4.

Criterion 9.1 – There are no FI secrecy laws that inhibit the implementation of AML/CFT measures in the Netherlands (including the BES Islands).

Access to information by competent authorities

The general provision for supervisors to obtain information is set out in General Administrative Law (Awb, Art. 5:16). Authorities are able to obtain information from any person necessary to exercise their functions (Wft, Art. 1(74)), but are prohibited from using confidential data (data that can be traced to an individual) collected through the course of their activities, or from a foreign supervisor, for any purpose other than carrying out their functions under the acts. Supervisors are also prohibited from sharing confidential information except where necessary to carry out their functions under the act (Wwft, Art. 22 (1)).

Other competent authorities, including LEAs, have statutory powers to request information from FIs (see R.29, R.31).

BES Islands: Supervisors are authorised to obtain information under the Wwft BES and BES Financial Markets Act. This includes power to enter premises and demand information (Wwft BES, Art. 5.5; Wfm BES, Art. 7.7–7.11).

Sharing of information between competent authorities

Supervisors are able to share confidential information obtained through the course of their activities with other domestic and foreign competent authorities (Wwft, Art, 22.a). There are no FI secrecy laws that inhibit this sharing.

BES Islands: Supervisors are authorised to share information obtained in the course of their duties with other competent authorities domestic or foreign, except in certain circumstances. This includes, where they have insufficient guarantees that the data or information will not be used for another purpose (Wwft BES, Art 1.5 (2-4)).

Sharing information between FIs

There are no secrecy laws that restrict the sharing of information between FIs, where this is required by R.13, 16 or 17. Subject to article 23 Wwft, FIs are required to share information regarding the reporting of an UTR within their financial groups (Wwft, Art, 23), unless the FIU-NL has indicated that this information must not be disclosed (Wwft, Art. 23a, 23(6)).

BES Islands: Information sharing within financial groups is permitted when such data and information relates to the prevention of ML and TF (Wwft BES, Art. 3.10).

Weighting and conclusion

All criteria are met.

Recommendation 9 is rated compliant.

Recommendation 10 – Customer due diligence

In its last MER, the Netherlands was rated partially compliant with the requirements of former R.5, as there were deficiencies in CDD measures for establishing BO and keeping CDD information up-to-date.

In Dutch law, only natural or legal persons can act in legal transactions. Trusts or similar legal arrangements can never be the customer in a legal transaction. In continental Netherlands, FIs are required to conduct CDD on a trust or similar legal arrangement (Wwft, Art. 3(3). There are deficiencies relating to the requirement to identify and verify the indirect customers of legal arrangements in the Netherlands and BES islands.

Criterion 10.1 – There is no explicit prohibition on FIs from keeping anonymous accounts or accounts in obviously fictitious names. Nevertheless, FIs are required to perform CDD before establishing a business relationship or conducting a transaction (Wwft, Art.5(1); Wwft BES, Art.2.4(2)). This includes obtaining and verifying the identity of the customer and, in the case of legal persons, the BO.

a) ***Criterion 10.2 –*** FIs are not permitted to enter into a business relationship unless CDD has been carried out (Wwft, Art.3(5); Wwft BES, Art.2.3(a)).

b) FIs must conduct CDD for occasional transactions in or from the Netherlands with a minimum value of EUR 15 000, whether the transaction is carried out in a single operation or in several operations that appear to be linked (Wwft, Art.3(5)(b)).

Technical compliance

BES Islands: FIs must conduct CDD on all occasional transactions (Wwft BES, Art2.4).

c) CDD must be conducted on transactions in or out of the Netherlands for customers above EUR 1 000, where these transactions are defined as transfers of funds in the Article 3.9 of Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds (Wire Transfer Regulation).

BES Islands: All wire transfers in and out of the BES Islands are subject to CDD (Wwft BES, Art. 2.3(1)(b)).

d) FIs are required to perform CDD if there are indications that the customer is involved in ML or TF (Wwft, Art.3(5)(c); Wwft BES, Art.2.3(c)).

e) FIs are required to perform CDD when there are doubts about the veracity or adequacy of previously obtained customer identification data (Wwft, Art.3(5)(d); Wwft BES, Art.2.3(d)).

Criterion 10.3 **–** FIs are required to identify and verify the customer's identity (Wwft, Art.3(2)(a) and 3.3; Wwft BES, Art 2.2(2)(a)). Identification must be verified using reliable and independent sources (Wwft, Art.11(1-3); Wwft BES, Art. 2.12(1) Wwft BES art. 2.2 (2)(b)).

Criterion 10.4 **–** FIs are required to establish whether any natural or legal person who represents the customer is authorised to do so, and identify and verify the identity of that person (Wwft, Art.3(2)(e); Wwft BES, Art.2.2(2)(e)-(f)).

Criterion 10.5 **–** FIs are required to identify BOs and take reasonable measures to verify their identity (Wwft, Art. 3(2)(b); Wwft BES, Art.2.2(2)(b)). Documents that can be used to fulfil this requirement are listed in the Wwft implementing regulation and include an extract from the Commercial register or a deed or declaration, drawn up or issued by a lawyer, civil-law notary, junior civil-law notary or comparable independent legal professional practising in the Netherlands or in another Member State (Art. 4(2); Wwft BES, Art. 2.12, 14 and BES ML/TF Regulation, Art 4.2).

Criterion 10.6 **–** FIs are obliged to understand and obtain information on the purpose and intended nature of the business relationship (Wwft, Art.3(2)(c); Wwft BES, Art.2.2 (2)(c)).

Criterion 10.7 **–** FIs are required to continuously monitor the business relationship. This includes:

a) monitoring all transactions performed over the course of the relationship, to ensure they are consistent with the institutions' knowledge of the customer and their business and risk profile, including where necessary, the source of funds (Wwft, Art.3(2)(d); Wwft BES, Art.2.2 (2)(d)).

b) ensure that all data collected in the context of CDD is kept up-to-date (Wwft, Art.3(11); Wwft BES, Art.2.2(6)). CDD must be performed by FIs in certain higher risk situations, for example, if there are indications the customer is involved in ML/TF, there are doubts about the accuracy of information previously obtained or if the risk of an existing customer's involvement in ML/TF gives cause to do so (Wwft, Art.3(5) Wwft BES, Art.2.3).

Criterion 10.8 **–** In the case of legal persons and legal arrangements, FIs are required to take reasonable measures to understand the customer's ownership and control structures. There is an explicit requirement for FIs to understand the nature of their customer's business and monitor the business relationship and transactions to ensure they align with their understanding of the customer's profile (Wwft, Art. 3.2(c)(d); Wwft BES, Art. 2.2(2)(d)).

Criterion 10.9 **–** FIs are required to identify customers that are legal persons or arrangements and verify their identity on the basis of documents, data or information from a reliable and independent source Wwft, Art 11(1). This includes:

a) An extract from the commercial register (if required to be registered with the CoC) or a deed or declaration by a lawyer, civil-law notary, junior civil-law notary or comparable, independent legal professional practicing in the Netherlands or in another Member State (Wwft, Art. 11(2); Wwft Regulation 2018, Art. 4(2)). For customers that are foreign legal persons, FIs must verify their identity on the basis of documents that are customary in international commerce or that have been recognised by the law as a valid means of identification in the State of origin of the customer. The information for all legal persons must include the name, legal form, and, if it is registered with the CoC, proof of existence through the registration number and the method by which the identity was verified (Wwft, Art Art.33(2)(c)(1)(2)).

b) If the customer acts as a trustee of a trust or other legal arrangement, CDD requirements apply and must enable the institution to establish whether the customer is authorised to act as trustee of a trust or for the benefit of another legal construct (Wwft Art 3 (2)(3)). In such cases, FIs must also collect information on the objective and nature of the trust or other legal construct and its governing laws. Legal persons and other legal entities established in the Netherlands must register with the CoC and obtain a registration number (Hrw, Art.9; Hrw BES, Art.5). Requirements to register include the details of directors and persons charged with the day-to day management of the business and the legal form (Hrw, Art.18). FIs may also collect information on senior management when performing other parts of CDD, including when determining the customer's ownership and control structure or when identifying the person acting on behalf of the customer.

c) The address of the registered office and a principal place of business (Wwft, Art.33(2)(c); Wwft BES, Art. 2.12)).

BES Islands: All legal persons need to be registered, including their owners and directors (Hrw BES, Art, 3-5). FIs are required to collect either a certified extract from the CoC or from a comparable foreign registry, or a deed or declaration drawn up by a lawyer or notary. This must include the name, legal form and registration number (Wwft BES, Art. 2.12, BES ML/TF Regulation, Art. 4(2-4)). FIs are required to identify and verify domestic and foreign legal persons on the basis of documents, data or information from a reliable and independent source. Foreign legal persons can be verified using similar documents recognised for identification in the country of origin (Wwft BES, 2.12(1).

Criterion 10.10 **–** FIs are required to identify and take reasonable measures to verify the BO of a legal person by collecting the following information:

(a)-(b) The identity of all natural persons that directly or indirectly ultimately own or control the company by holding shares or voting rights that exceed 25% of the company and natural persons who have actual control over the legal entity (i.e., hold a decision making position) (Wwft Decree, Art. 3; Bwft BES, Art. 2).

c) In case no natural person is identified, or there is doubt as to whether the person referred to under (a) and (b) is the BO, the identity of the natural person belonging to the senior management of the legal person (Wwft Decree, Art. 3; Bwft BES, Art. 2).

Criterion 10.11

a) FIs are required to identify and take reasonable measures to verify the identity of BOs of trusts including the settlor(s), trustee(s), protector(s) and beneficiaries (where it is not possible to identify the beneficiaries, the class of person in whose main interest the trust is set up in or operates) and any other natural person who ultimately controls the trust (Wwft Decree 2018, Art.3(1)(e); Bwft BES Art. 2(1)(d)).

b) The obligations to perform CDD also apply to other legal arrangements (Wwft Decree 2018, Art.3(5); Bwft BES, Art. 2(5)).

Criterion 10.12 – In relation to life insurance policies, FIs are required to conduct CDD as soon as the beneficiary is identified or designated. This includes:

a) registering the name of the person, if the beneficiary is a natural person or legal person or legal construct mentioned by name (Wwft, Art.3a; Wwft BES, Art.1.1(b) and Art.2.7(2));

b) obtaining sufficient information concerning the beneficiary to become satisfied that the identity of the beneficiary can be established at the time a payment when the beneficiary has been designated by characteristics, by class, or by other means. For the BES Islands, this must take place at or before the time of payment, or at or before the time when the beneficiary wants to exercise his rights under the policy (Wwft 3a(1)(b); Wwft BES, Art.2.7);

c) verifying the identity of the beneficiary at the time of the payout (Wwft, Art.3a(1)(b); Wwft BES, Art.2.7).

Criterion 10.13 **–** FIs must adapt CDD measures based on the ML/TF risks of their customers, business relationships, products or transactions (Wwft, Art.3(8); Wwft BES, Art.1.8 and 2.2). If the business relationship or transaction entails a greater risk of ML/TF, enhanced measures must be applied. The inclusion of both 'business relationship' and 'transactions' also covers life insurance beneficiaries (Wwft, Art. 8.1(a) Wwft BES, Art 1.1(b)).

Criterion 10.14 **–** FIs must identify customers and BOs when establishing a business relationship or carrying out an occasional transaction. FIs are permitted to verify the identity of the customer and BO after entering the business relationship if this is necessary to avoid disruption, provided that this is done as soon as possible after the first contact with the customer and the risk of ML/TF is low (Wwft, Art.4(3); Wwft BES, Art.2.7(1)).

Criterion 10.15 **–** FIs are required to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification (Wwft, Art. 2c(1); Wwft BES, Art. 1.10(1))

Criterion 10.16 **–** FIs are required to continuously monitor customer relationships and apply CDD to existing customers in the situations referred to in c.10.2, including on the basis of ML/TF risks (Wwft, Art.3(5)(e); Wwft BES Art.2.3(1)(c). Monitoring must be based on the risk profile of the customer. Customer data must be kept up to date (Wwft, Art. 3(8); Wwft BES, Art.2.2 (6). There are requirements to check if customers who existed before legislative changes meet requirements (e.g. AMLD4 and the revised Wwft BES), but there are no other specific requirements for existing customers.

***Criterion 10.17* –** FIs must perform EDD where higher risks are identified (Wwft, Art. 8(1); Wwft BES, Art. 2.10(1)).

Criterion 10.18 FIs are permitted to perform simplified CDD when the risk of ML/TF is low. In such cases, FIs must demonstrate that sufficient information was gathered to determine that simplified measures are appropriate (Wwft, Art. 6.2; Wwft BES, Art.2.8 (1)(2)). EDD must always be applied if the business relationship or transaction entails a greater risk of ML/TF, or if it involves a customer from a jurisdiction designated as higher risk for ML/TF by the EC (Wwft, Art.8(1)(a); Wwft BES, Art.2.10(1).

***Criterion 10.19* –**

a) FIs are not permitted to enter into a business relationship or conduct a transaction for a customer until CDD has been carried out. Verification of identity can take place after the business relationship is established to avoid disruption, where there is low risk and provided verification takes place at the first opportunity. Where a business relationship has already been established, FIs are required to terminate the business relationship if it is unable to comply with CDD measures (Wwft, Art.5(3); Wwft BES, Art. 2).4). FIs can also open accounts (including securities accounts) providing these cannot be used before verification has taken place and in the case of trust and legal persons, before the beneficiary exercises their definitive rights (Wwft, Art.4(4); Wwft BES, Art.2.7(1)(3)).

b) FIs must submit a UTR when the unusual nature of the transaction becomes known, including when a relationship is terminated or if there is an indication the customer is involved in ML/TF (Wwft, Art.16.1, 16.4(b); Wwft BES, Art.3.5, 3.5(4)b).

***Criterion 10.20* –** FIs and their employees are obliged to maintain confidentiality on UTRs submitted to the FIU (Wwft, Art. 23(1). This obligation has priority over other obligations. The Wwft does not, in any way, obstruct the performance of CDD being postponed or abandoned if this would lead to the customer being tipped off. OM can request information from an FI and indicate in the demand that it does not want the customer to know of an investigation. It can also request that the customer relationship and transactions be maintained until indicated otherwise (DNB Guidance, p.59 and Explanatory Memorandum of the Wwft). In such cases, the requirement to submit an UTR remains.

Weighting and Conclusion

While most of the CDD measures meet the FATF Standards, there is there is no specific requirement for FIs to take into account when previous measures have taken place when applying CDD to existing customers, other than if this took place before the implementation of AMLD4 or the equivalent measures in the Wwft BES. This is a minor deficiency.

Recommendation 10 is rated largely compliant.

Recommendation 11 – Record-keeping

In its last MER, the Netherlands was rated as LC with the previous R.10 because of ambiguity around the time required to retain records, a lack of explicit requirement that records of transactions should be sufficient to permit reconstruction of transactions sufficient for a prosecution and a lack of power to extend the retention period if necessary.

Criterion 11.1 – FIs are required to perform CDD to enable them to continuously monitor the business relationship and the transactions conducted during the period of that business relationship (Wwft, Art. 3(2)(d); Wwft BES, Art. 2.2(2)(d)). Documents and data used in the course of performing CDD must be retained for five years after the date of termination of the business relationship or up to five years after completion of the relevant transaction (Wwft, Art. 33(1) and (3); Wwft BES). In the BES Islands, there is no similar requirement for this information to be retained on all transactions, as it is not covered by the requirements on the types of information that must be retained (Wwft BES, Art. 2.2 and 2.13).

Criterion 11.2 – FIs are required to retain all CDD records for a period of five years after the date of termination of the business relationship or after the completion of the relevant transaction (Wwft, Art.33(1) and (3)). Additionally, FIs must maintain all business records for seven years (AWR, Art.52; BES Tax Act, Art.8.86). However, this only includes the information referred to in Annex B of the Wwft BES Act, which does not cover all information as required by c.11.2 including transaction records or correspondence.

Criterion 11.3 – FIs must retain the documentation and information referred to in c.11.1 in a retrievable format. In relation to UTRs, FIs are required to retain all data necessary for the reconstruction of a transaction for a period of five years from when the UTR was submitted. The submitting FI must also retain a copy of the submitted report and the notification of receipt from the FIU (Wwft, Art 34; Wwft BES, Art. 3.5(3)).

Criterion 11.4 – FIs are required to ensure that CDD information and transaction records on UTRs are kept in an accessible manner and have systems in place to promptly respond to requests from the FIU and supervisors (Wwft, Art. 33(3), 34(1); Wwft BES, Art. 2.13, 3.5(3)).

Weighting and Conclusion

FIs in the BES are not required to retain all information required by c.11.2 including transaction records or correspondence. This is a minor deficiency.

Recommendation 11 is rated largely compliant.

Recommendation 12 – Politically exposed persons

In its last MER, the Netherlands was rated partially compliant with the requirements of former R.6. Deficiencies related to requirements to determine PEPs' source of wealth, foreign PEPs residing in the Netherlands requirements and senior management approval for existing business relationships. In addition, the definition of close associate only covered those who were "publicly known".

Criterion 12.1 – PEPs are defined as any natural person who holds or has held a prominent public function, designated by order in council (Wwft, Art. 1.1), or holds or has held a prominent office within or outside the public bodies in the BES islands

(Wwft BES, Art. 1.1(o)). There is no distinction between foreign and domestic PEPs in the Netherlands and the same measures that apply to domestic PEPs apply to foreign PEPs.

In addition to performing CDD as set out in R.10, FIs are required to:

(a) have appropriate risk management systems, including risk-based procedures in place to determine whether the customer or BO is a PEP (Wwft, Art. 8(5)(a); Wwft BES, Art. 2.10(3));

(b) obtain senior management approval when establishing or continuing a business relationship or conducting a transaction for a PEP (Wwft, Art. 8(5)(b)(1)). In the BES Islands, the decision is taken by a person approved by the service provider. There is no requirement on the level of seniority of the approved person (Wwft BES, Art. 2.10(3)).

(c) take appropriate measures to establish the source of assets and funds used in the business relationship or transaction (Wwft, Art. 8(5)(b)(2)). In the BES Islands, FIs are only required to establish the source of assets (Wwft BES, Art. 2.10(3)(b)).

(d) subject the business relationship to increased monitoring (Wwft Art, 8(5)(b)(3); Wwft BES, Art. 2.10(3)(c)).

Criterion 12.2 – FIs must apply the same measures outlined in c.12.1 to domestic and foreign PEPs, including taking reasonable measures to determine if the customer of a BO is a PEP and adopting the measures in 12.1(b) to (d)).

Criterion 12.3 – Measures set out in criterion 12.1 and 12.2 also apply to family members and close associates of PEPs (Wwft, Art. 8(8); Wwft BES, Art. 1.1(1)(o)).

Criterion 12.4 – FIs are required to take appropriate measures to determine if the beneficiary or the BO of the beneficiary of a life insurance policy is a PEP. In such situations, senior management must be informed prior to the payment of the proceeds of the policy and the entire business relationship must be subject to increased monitoring (Wwft, Art. 8(6)). While there is no specific requirement to file a UTR when higher risks are identified, the general requirement to report UTRs applies (see R.20).

BES Islands: FIs are required to apply the measures in c.12.1-12.3 to all customers, including persons on whose behalf a transaction is carried out. In the event of paying the benefits pursuant to a life insurance contract, this includes both the person who pays the premium and the beneficiaries (Wwft BES, Art. 1.1(1)). FIs are required to verify the identity of the beneficiary of a policy before the payment, or at or before the time when the beneficiary exercises their rights under the policy (Wwft BES, Art. 2.7). There is no requirement to inform senior management before payout. However, FIs are required to obtain senior management approval prior to establishing the business relationship.

Weighting and Conclusion

FIs must obtain senior management approval when establishing or continuing a business relationship or conducting a transaction for a PEP. There is no strict requirement to have senior management approval for establishing and continuing PEP relationships in the BES Islands. This function can be designated to a person authorised by the FI, but there are no requirements for this person to be senior. FIs are required to determine source of assets when establishing or continuing a relationship with PEPs. FIs in the BES Islands are not required to establish the source of funds and there is no express requirement to inform senior management before the payout of life insurance policies.

Recommendation 12 is rated largely compliant.

Recommendation 13 – Correspondent banking

In its last MER, the Netherlands was rated largely compliant with the requirements of former R.7. Deficiencies related to the application of EDD to FIs headquartered in EU Member States and there were no enforceable means in the case of pay-through accounts.

Criterion 13.1 **–** FIs in the Netherlands must apply CDD measures to every customer, including correspondent banking relationships (Wwft Art, 3). For cross-border correspondent banking relationships this includes:

a) collecting sufficient information about the relevant respondent institution in order to obtain a complete picture of the nature of its operations. The FI should use publicly available information to assess the reputation of the respondent institution and the quality of its supervision.

b) assessing the procedures and measures implemented by the relevant respondent institution to prevent ML and TF.

c) obtaining senior management approval prior to entering into a correspondent banking relationship

d) defining the responsibilities of both credit institutions (Wwft, Art.8(4) a-d; Wwft BES, Art.2.11(a-d)).

In the continental Netherlands, however, these provisions only apply to situations where the respondent institution is outside the EEA. For correspondent banking relationships within the EEA, a risk-based approach is taken (Wwft, Art. 8(1)). However, this is not in line with R.13, which requires that the above measures be applied to all cross-border correspondent banking relationships.

Criterion 13.2 **–** Regarding payable-through accounts, FIs must satisfy themselves that:

a) the respondent bank has identified the customers who have direct access to transit accounts and has verified their identity, that it constantly monitors these customers;

b) they are able to obtain relevant customer information upon request (Wwft, Art. 8.4(e); Wwft BES, 2.11(e)).

However, the requirements in the Netherlands only apply to correspondent banks outside the EEA.

Criterion 13.3 **–** FIs are prohibited from entering into or continuing a correspondent banking relationship with a shell bank or an FI known to permit shell banks from making use of its accounts (Wwft, Art. 5(5); Wwft BES, Art. 4.22)).

Weighting and Conclusion

FIs are required to take steps in line with R.13 for cross-border correspondent banking relationships. However, the mandatory EDD measures regarding correspondent banking relationships apply only to respondent institutions outside the EEA. Even though similar deficiencies are not present in the BES Islands, deficiencies in the continental Netherlands have been given significant weight as the majority of the corresponding banking relationships exist within the EEA.

Recommendation 13 is rated partially compliant.

Recommendation 14 – Money or value transfer services

In its last MER, the Netherlands was rated largely compliant with the requirements of former SR.V1. The same deficiencies identified in relation to the FI sector, applied to MVTS (e.g., CDD measures for BO and keeping CDD information up-to-date).

Criterion 14.1 **–** MVTS are carried out by payment services providers, electronic money institutions and banks. DNB licences institutions carrying out MVTS services under the provisions of the Wft Art.2:3a (payment services providers), 2:10a (electronic money institutions) and 2:12 (banks); Wfm BES, Art 2:1.

Criterion 14.2 **–** Obliged entities carrying out MVTS must register with the DNB. Carrying out MVTS activity without a licence is an economic offence that carries a fine up to EUR 87 000, four years imprisonment or community service (WED, Art. 6). Agents of MVTS providers must be notified to the authorities by the MVTS provider. Obliged entities providing MVTS in the BES Islands must be licenced before carrying out this activity (Wfm BES, Art. 2:1). Operating without a licence can be punished with imprisonment of up to five years or a fine of the fifth category (up to USD 560 00) (Wfm BES, Art. 9:1).

Criterion 14.3 **–** MVTS are regulated as other financial undertakings and are subject to AML/CFT supervision by DNB (see R.26).

Criterion 14.4 **–** MVTS providing payment services through the use on an agent must notify DNB and provide the agent's details. If the details are confirmed to be accurate by DNB, the agents are listed on a register (Wft, Art. 2.3c). MVTS activity in the BES islands can only be carried out by money transfer offices, which must be licensed (Wfm BES, Art. 2:1) Money transfer companies in the BES Islands must maintain a list of their agents and branches and subsidiaries.

Criterion 14.5 **–** Agents of MVTS providers are subject to the requirements of the Wwft (Wwft, Art. 1a (3)(j), including ensuring that their employees are aware of the AML/CFT requirements and that they receive periodic training to recognise an unusual transaction and carry out proper and complete CDD (Wwft, Art. 35; Wwft BES, Art. 3.12).

Weighting and conclusion

All criteria are met.

Recommendation 14 is rated compliant.

Technical compliance

Technical compliance

Recommendation 15 – New technologies

In its last MER, the Netherlands was rated largely compliant with the requirements of former R.8. There was no specific obligation to prevent the misuse of new technology and potential shortcomings in provisions for ensuring effective CDD procedures in the case of non-face-to-face transactions. Requirements on new technology have since been amended to include new requirements relating to VAs. The Netherlands has introduced measures to mitigate the risks associated with VAs. However, the definition of VASPs is limited to two of the five activities included the FATF definition of VASPs (custodian wallets and exchanging VAs for fiat currency) (Wwft, Art.1a(4)(l) and (m)). This has a significant impact on a number of requirements in R.15, particularly on registration, monitoring, mitigation measures, and the application of enforcement measures. The Netherlands has assessed the risk of VA in the BES Islands as low on the basis that no VASPs operate on the islands. Notwithstanding, there are no requirements for VASPs in the BES Islands to implement preventative measures, or for supervisory authorities to license/register and supervise VASPs.

Criterion 15.1 **–** The Netherlands is required to produce an NRA every two years (Wwft, Art.1f). The most recent assessment includes risks associated with new technologies (Wwft, Art.1f). In the BES Islands, authorities are required to periodically publish an NRA (Wwft BES, Art.1.14). The latest 2021 BES NRA suggested that virtual currencies are not an ML risk.

FIs are required to take measures to identify and asses its ML/TF risks, and *inter alia* take into account the risk factors related to the type products, services, transactions and channels of supply (see c.1.10; Wwft, Art.2b); Wwft BES, Art.1.9).

Criterion 15.2 **–** FIs are required to:

a) keep updated risks assessments, which must take into account the risk factors related to the type of product, service and delivery channel (Wwft, Art. 2b(2) and (3); Wwft BES, Art. 1.9(3). There is no specific obligation to analyse the risks before products are launched, but it is not possible to fulfil the obligations in Art Wwft 2b (1-3) without analysing the risks beforehand.

b) have in place policies, procedures and measures to mitigate and effectively manage the risks of ML and TF (Wwft, Art. 2c; Wwft BES, Art. 1.10). Additionally, FIs are required to take adequate measures to prevent ML/TF risks originating as a result of new technologies (Wwft, Art.2a(2); Wwft BES, Art.1.8(2)).

Criterion 15.3 **–** In line with R.1, the Netherlands has:

a) Identified and assessed the risks of VAs and covered VASPs in the NRA, particularly risks arising from anonymous transactions. VAs are assessed as part of the NRA in the BES Islands, although no risks have been found.

b) Covered VASPs are obliged entities and subject to the requirements of the Wwft (Wwft, Art.1a(4)(l) and (m)). DNB is the competent authority for supervising VASPs compliance and is required to supervise in a risk-based and effective manner, taking into account Article 48(6) to (8) of AMLD4 (Wwft, Art.1d(6)). There are no requirements for VASPs in the BES islands.

c) Covered VASPs are subject to the same requirements as FIs other than financial undertakings as defined in the Wwft. They are required to take appropriate steps to identify, assess, manage and mitigate their ML/TF risks as set out in c.1.10 and 1.11 and are subject to the same deficiencies. These requirements do not apply to VASPs in the BES islands.

The definition of VASPs is limited to two of the five activities included the FATF definition of VASPs. This is a major deficiency.

Criterion 15.4 –

a) Natural and legal persons that provide VASP activities covered by Dutch legislation are required to register with DNB if they:

i. offer professional or business services in or from the Netherlands for exchanging VA and fiduciary currency.

ii. offer professional or business services for virtual asset wallets in or from the Netherlands (Wwft Art, 23b).

The obligation to register with DNB extends to parties established in the Netherlands and abroad but operating in the Dutch market. It is prohibited for anyone residing or established in a third country to offer professional or business services for exchanging VA and fiduciary currency or virtual asset wallets (Wwft, Art. 23g).

b) Covered VASPs are subject to fit and proper requirements designed to prevent criminals or their associates from holding, being the BO of a significant or controlling interest, or holding a management function in a VASP (Wwft, Art. 23(h)1-4).

***Criterion 15.5* –** Failure by covered VASPs to register with DNB when carrying out the activities in c.15.4a can result in proportionate and dissuasive sanctions (see R.35 for violations of the Wwft). DNB has carried out measures to identify covered VASPs operating without a license, including a "webscraping" exercise.

***Criterion 15.6* –** DNB is the competent authority for the registration and supervision of covered VASPs (Wwft, Art.1d(1)(a)). DNB is required to fulfil its task risk-based and effectively (Wwft, Art.1d(6)). DNB has powers to supervise and ensure covered VASPs compliance with AML/CFT requirements (Awb, Ch. 5). These powers are the same as those available for FIs (see R.27) and include the power to cancel registration in the case of non-compliance with the Wwft or Sw (Wwft, Art. 23d (3)).

***Criterion 15.7* –** FIU-NL has appointed a relationship manager for the VASP sector. The relationship manager provides information to the covered VASPs on a continuous basis and regularly attends meetings with the private sector. The relationship manager provides information sessions (such as seminars/webinars), newsletters and case examples to the private sector and is in regular contact with the supervisory authorities.

BES islands: the FIU-NL monitors the transactions on the BES that can be related to VASPs. The FIU-NL informs the obliged entities and the chain partners on the BES Islands about certain red flags, signals related to VASPs.

DNB provides guidance on the obligations for covered VASPs, including on transaction monitoring and reporting duties. In 2018 and 2019, DNB organised seminars for VASPs and in 2020, organised a webinar on TFS compliance.

***Criterion 15.8* –** Competent authorities have a range of sanctions available, including the ability to impose administrative and criminal sanctions and withdraw, restrict or suspend a registration (see c.15.5).

Technical compliance

Criterion 15.9 Covered VASPs are subject to the requirements set out in R.10-21 in the same manner as FIs, and are subject to the same deficiencies.

a) For occasional transactions, CDD must be conducted where the transaction is over EUR 15 000 for non-commercial customers (Wwft, Art. 3), this is a significant departure from the FATF threshold of EUR 1 000.

b) For virtual asset transfers by entities defined as VASPs in the Netherlands:

(i) Both originating and beneficiary covered VASPs must conduct CDD under Article 3 Wwft, thereby obtaining the information referred to in c.16.1.a. This information must be retained for up to five years after the end of the relationship (Wwft, Art. 33(3).

(ii) VASPs must retain the information such that they can immediately respond to requests from competent authorities (Wwft, Art.33(4)).

(iii) VASPs are required to freeze the economic resources of sanctioned persons and ensure the funds and economic resources are not made available. In such cases, VASPs must notify the DNB of the frozen funds (Sw, Art.10(2) l and m). The term 'funds and other resources' also covers VAs.

(iv) VASPs are subject to the same obligations that apply to other FIs when sending or receiving VA transfers on behalf of a customer.

Criterion 15.10 – TFS communication mechanisms in c.6.5(d), 6.6(g), 7.2(d) and 7.4(d) apply equally to covered VASPs.

Criterion 15.11 – The Netherlands has mechanisms in place to provide international co-operation (see R.37-49). The mechanisms for international co-operation described in R.37-40 apply to ML/TF through VA. DNB can exchange information about covered VASPs in the same way it exchanges information about other obliged entities (see c.40.12-16).

Weighting and Conclusion

The Netherlands employs a definition of VASPs, which only applies to VA to fiat transactions (and vice versa) and custodian wallets. This definition does not cover all activities included in the FATF definition, such as the exchange between one or more forms of VAs. This is a significant technical deficiency. Furthermore, there is no regime for VASPs in the BES Islands and the threshold for the application of CDD measures for occasional transactions is higher than the threshold in the FATF Standards. These deficiencies are heavily weighted by the Assessment Team and significantly impact the overall rating of R.15.

Recommendation 15 is rated as partially compliant.

Recommendation 16 – Wire transfers

In its last MER, the Netherlands was rated compliant with the requirements of former SRVII.

Criterion 16.1 – FIs are required to ensure that all cross-border wire transfers over EUR 1 000 or more are accompanied by: (a) the required and accurate originator information (name, account number, address, official personal document number, customer ID number or date and place of birth), and; in the Netherlands (b) beneficiary information (name and account number) (EU Regulation 2015/847, Art.4; Wfm BES, Art 4:19(1), Rfm BES, Art, 3.5)). If the transaction is not made from/to a payment account, a unique transaction identifier is required rather than the account number (EU Regulation 2015/847, Art.4(3)). There are no requirements on beneficiary information for FIs in BES Islands.

Criterion 16.2 The requirements in the Netherlands regarding batch files are consistent with the FATF requirements regarding originator and beneficiary information (EU Regulation 2015/847, Art.6(1); Rfm BES, 3:7).

BES Islands: The requirements regarding batch files do not extend to information on the beneficiary.

Criterion 16.3 – A *de minimis* threshold of EUR 1 000 applies to the application of requirements in c.16.1. The requirements for the originator and beneficiary information accompanying all transfers below EUR 1 000 are consistent with the FATF Standards (EU Regulation 2015/847, Art.6(2)).

BES Islands: FIs are required to carry out CDD on all occasional transactions including cross-border transactions. There are no requirements to provide the beneficiary information stipulated in c.16.3 (Wwft BES, 2.3 (1)(b)).

Criterion 16.4 - For transfers of less than EUR 1 000, originator information must be verified where there are reasonable grounds for suspecting ML/TF, or the funds were received in cash or anonymous e-money (EU Regulation 2015/847, art.6(2)); Wwft BES, Art. 2.3(c-d)).

BES Islands: There is a general provision for FIs to investigate clients if there are indications of ML/TF or if there are doubts about the reliability of the information provided.

Criterion 16.5 and 16.6 – For domestic wire transfers (which in this case also includes intra-EU wire transfers), ordering FIs need to provide only the payment account numbers (or unique transaction identifiers) with the transfer. The ordering FI must be able to provide complete information on the originator and the beneficiary, if requested by the beneficiary FI, within three working days which is consistent with the second part of c.16.5 and c.16.6. There is also a general obligation for FIs to respond to requests from authorities on originator and beneficiary information (EU Regulation 2015/847, arts.5, 14). FIs are also obliged to appoint a central point of contact.

BES Island: FIs are only required to provide the account number or unique identifier for domestic transfers (Rfm BES, 3:6(3)). In such cases the payment service provider of the payer is required to make available complete information on the payer to the FI of the beneficiary, no later than three working days after receipt of the request (Rfm BES, Art. 3.6(4)). FIs are required to have procedures in place to ensure that it can provide the information on the payer without delay to supervisors (Rfm BES, Art. 3:14).

Criterion 16.7 – Ordering and beneficiary FIs are required to retain information on the originator and, in the Netherlands, the beneficiary for five years (EU Regulation 2015/847, Art.16; Rfm BES, Art. 3.6(2), 3:11)).

***Criterion 16.8* –** The ordering FI is not allowed to execute the wire transfer if it does not comply with the requirements set out in c.16.1-16.7 (EU Regulation 2015/847, Art.4(6)).

BES Islands: Beneficiary FIs are required to refuse transfers of funds if information on the payer is incomplete (Rfm BES, Art. 3:10). This does not apply to beneficiary information.

***Criterion 16.9* –** An intermediary FI must retain with the cross-border wire transfer all accompanying originator and beneficiary information (EU Regulation 2015/847, Art.10).

BES Islands: Intermediary FIs are required to ensure that information about the payer remains with the transfer (Rfm BES. Art 3:12). This does not apply to beneficiary information.

***Criterion 16.10* –** FIs are not able to use 'technical limitations' to justify non-compliance with c.16.9.

BES Islands: Where an intermediary payment service provider uses a payment system with technical limitations, it must retain the information for a period of five years (Rfm BES, Art 3:13(2)). However, there is no requirement for beneficiary information.

***Criterion 16.11* –** Intermediary FIs are required to take reasonable measures that are consistent with straight-through processing, to identify cross-border wire transfers that lack originator or beneficiary information (EU Regulation 2015/847, Art.11).

BES Islands: There are no requirements for intermediaries to take reasonable measures that are consistent with straight-through processing, to identify cross-border wire transfers that lack beneficiary information.

***Criterion 16.12* –** Intermediary FIs are required to have risk-based procedures for determining: (a) when to execute, reject, or suspend a wire transfers that lack the required originator and beneficiary information; and (b) for taking the appropriate follow-up action (EU Regulation 2015/847, Art.12).

BES Islands: Where a payment service provider receives a transfer with incomplete payer information, it must refuse a transfer until it has received the missing details (Rfm BES, Art. 3:10). Intermediaries are required to have measures in place to consider whether to limit or terminate its relationship with a service provider if it regularly fails to provide he required information about the payer (Rfm BES: Art 3:8). However, these requirements do not extend to information on the beneficiary.

***Criterion 16.13* –** The beneficiary FI is required to detect whether the required information on the originator or beneficiary is missing (EU Regulation 2015/847, Art.7).

BES Islands: The payment service provider of the beneficiary must check whether the fields for information on the payer in the messaging system or the payment and settlement system used for the transfer of funds have been completed (Rfm BES, Art. 3:9).

***Criterion 16.14* –** The beneficiary FI is required to verify the identity of the beneficiary of cross-border wire transfers of over EUR 1 000 and maintain this information for five years (EU Regulation 2015/847, Art.7, 16; Rfm BES, Art. 3:11).

***Criterion 16.15* –** Beneficiary FIs are required to have risk-based policies and procedures for determining: (a) when to execute, reject or suspend a wire transfer lacking originator or required beneficiary information; and (b) the appropriate follow up action (including reporting to authorities in cases of routine failure to provide information) (EU Regulation 2015/847, Art.8).

BES Islands: The FI of the beneficiary must have procedures and measures in place to consider whether or not to limit or terminate its relationship with the ordering or intermediary FI, if it regularly fails to provide the required information about the originator (Rfm BES, Art. 3.8). This does not extend to beneficiary information. There is also no requirement for the procedures and measures to be risk-based or to include adequate appropriate follow-up action, including to consider filing a report to authorities.

Criterion 16.16 – The obligations listed above also apply to MVTS providers and their agents in the continental Netherlands (EU Regulation 2015/847, Art. 2(1)).

BES Islands: MVTS providers are subject to the same requirements as FIs in relation to CDD. The deficiencies highlighted throughout R.16 also apply to MVTS.

Criterion 16.17 –

a) EU Regulation 2015/847 requires all payee and intermediary institutions to take into account information from both sides as a factor when assessing whether an UTR should be filed.

b) While there is no explicit requirement for the MVTS provider to file a UTR/STR in any country affected by the transaction, taking into account 16.17(a) and the EU permissions for intra-group sharing of STR data (see 18.2(b)), MVTS providers are obliged to report in the countries of the ordering and beneficiary sides of the transaction. In addition, relevant to EU passporting, compliance officers must file an UTR/STR with the FIU of the EU Member State in whose territory the MVTS provider is established (i.e., its headquarters) (EU Directive 2015/849, Art. 33).

BES Islands: MVTS providers are subject to the same requirements as FIs in relation to CDD including the submission of UTRs.

Criterion 16.18 – All natural and legal persons in the Netherlands, including FIs, are required to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities when conducting wire transfers (see R.6).

Weighting and Conclusion

Requirements are implemented through EU Regulation, which covers most of the requirements for wire transfers. There are no requirements for FIs in the BES Islands to send beneficiary information for batch transfers and FIs of beneficiaries are not required to have risk-based procedures and measures in place where originator information is regularly not provided. These deficiencies are not weighted heavily due to the small size of the financial sector in the BES Islands.

Recommendation 16 is rated largely compliant.

Recommendation 17 – Reliance on third parties

In its last MER, the Netherlands was rated non-compliant with the requirements of former R.9. There were no requirements for the relying FI to retain ultimate responsibility for the CDD carried out by the third party or to obtain CDD records from the third party. FIs were not required to be satisfied that third parties were regulated or supervised.

***Criterion 17.1* –** FIs are not permitted to enter into a business relationship or carry out an occasional transaction unless the CDD measures required in R.10 (a)-(c) have been carried out (Wwft, Art.3(5); Wwft BES, Art.2.3). FIs can rely on third parties to conduct these CDD measures, provided the third parties are regulated under the Wwft or equivalent legislation (Wwft, Art.5(1); Wwft BES, Art. 2.6). The types of third parties that an FI may rely on are listed in the Wwft (Art. 5.1(a)1-5); Wwft BES, Art. 2.6).

- **a)** FIs are required to have all identification and verification data and other relevant documentation regarding the identity of the persons before entering a business relationship or carrying out an occasional transaction (Wwft Art 5.1(c); Wwft BES, Art.2.6).
- **b)** There are no specific provisions requiring FIs to satisfy themselves that relevant documentation relating to CDD will be available upon request from a third party. However, FIs must have all identification and verification data and other relevant documentation regarding the identity of the customer and where applicable, the BO, in its possession before entering into a relationship or carrying out a transaction (Wwft Art, 5.1(c); Wwft BES, Art. 2.4 (2)(c)).
- **c)** FIs can only rely on third parties that are subject to equivalent AML/CFT legislation. Equivalence only applies for obliged entities in the Netherlands, entities regulated for AML/CFT purposes in other EU and EEA Member States, entities in States outside the EU designated by the Minister of Finance, and obliged entities that form part of a group that complies with Dutch AML/CFT requirements (Wwft, Art. 5(1)). The reliant FI must satisfy itself that third parties are supervised or have measures in place to comply with CDD and record-keeping obligations.

BES Islands: FIs can only rely on CDD carried out by a collective investment scheme, life insurer, broker in life insurance, lawyers and notaries, credit institution or money transaction office that has been issued a license pursuant to the Financial Markets (BES Islands) Act and is supervised by DNB or AFM. Other enterprises or categories of institutions designated by Governmental Decree can also be relied on, but none have been designated to date (Wwft BES, Art. 2.6).

***Criterion 17.2* –** FIs are in certain cases permitted to rely on obliged entities established within the EU/EEA. Reliance on obliged entities from EU states is not based on ML/TF risks, but reflects the presumption that all EU member states implement all harmonised AML/CFT provisions. Reliance can also be placed on obliged entities in a state designated by the Minister of Finance (Wwft, Art. 5.1(a)(3)-(4)). There have been no designations to date.

BES Islands: It is not possible to rely on institutions that are not established on the BES Islands (Wwft BES, Art. 2.6 (a)).

***Criterion 17.3* –** FIs are permitted to rely on third parties that are part of the same group (obliged entities in the Netherlands, or foreign branches or majority-owned subsidiaries) that fully comply with the policies and procedures applicable at group-level, provided the following conditions are met:

a) the group complies with obligations in the Wwft, which includes R.10-12 and 18 (Wwft, Art. 5(2)(b));

b) the group applies CDD measures, record keeping rules and AML/CFT programmes at group level, which is supervised by a competent authority in an EU Member State or other state designated by the Minister of Finance (Wwft, Art. 5(2)(b)-(c));

c) FIs are only able to rely on third parties in the Netherlands, other EU member states, or non-Member States that have equivalent CDD measures and there is supervision of compliance with those provisions, or a branch of the institution in the Netherlands if designated by the Minister of Finance.

BES Islands: There are no provisions that allow entities part of a financial group to rely on each other. Accordingly, this criterion is not applicable.

Weighting and Conclusion

FIs are permitted to rely on regulated third parties. There is no provision requiring the reliant FI to satisfy itself that third parties are supervised or have measures in place to comply with CDD and record-keeping obligations, however, FIs are required to have CDD information in their possession before entering into a relationship or carrying out a transaction. Deficiencies exists stemming from the assumption that all EU member states apply adequate AML/CFT controls.

Recommendation 17 is rated largely compliant.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its last MER, the Netherlands was rated partially compliant with former R.15 and R.22. Deficiencies related to requirements on internal controls not being fully applicable to all FIs; employee training being limited in scope; no provision requiring FIs to apply Dutch standards to branches and subsidiaries in the EU or EEA; requirements to apply Dutch standards only applied to CDD and not to all AML/CFT measures.

Criterion 18.1 **–** FIs are required to have in place policies, procedures and measures, proportionate to their size, to mitigate and effectively manage the risks of ML and TF (Wwft, Art. 2c; Wwft BES, Art. 1.10). These include:

(a) Having an independent and effective compliance function, where appropriate to the nature and size of the FI. This includes the appointment of a compliance officer, insofar as the FI has two or more senior managers. (Wwft, Art. 2d(1-2); Wwft BES, Art. 1.11 (1-2)).

(b) Ensuring that employees are screened as relevant to their duties and taking into account the risks, nature and size of the FI (Wwft, Art. 35; Bfm BES, Art 3.16). Screening is not required in the BES Islands.

(c) Ensuring that employees are aware of their AML/CFT obligations and receive periodic training to recognise unusual transactions and to carry out proper CDD (Wwft, Art. 35; Wwft BES, Art. 3.12).

(d) Where applicable, and appropriate to the nature and size of the FI, having an independent audit function to monitor compliance with the Wwft and the performance of the compliance function (Wwft, Art. 2d(4)). FIs are responsible for determining if it is appropriate to have an audit function and guidance has been provided by the authorities to help determine this. There is no obligation for FIs in the BES islands to have an independent audit function.

Criterion 18.2 –

(a) FIs are required to ensure policies, procedures and measures to manage the risk of ML/TF are effectively applied by their branches or majority owned subsidiaries with offices outside the Netherlands (Wwft, Art. 2f(2); Wwft BES, Art. 1.12(2)). FIs that are part of a group are required to effectively implement the policies and procedures applicable at group-level in so far as they comply with the Wwft (Wwft, Art. 2f(1); Wwft BES, Art. 1.12). Group wide measures include policies and procedures on information sharing within the group, to the extent that such data and information relate to the prevention of ML and TF (Wwft Art. 2f(3); Wwft BES, Art. 1.12(3)).

(b) The policies and procedures required by Wwft Art, 2f must include provisions on data protection and policies and procedures for group-wide information sharing, to the extent that such data and information relate to the prevention of ML and TF. FIs in the Netherlands are required to share information on UTRs within the group, unless the FIU-NL provides otherwise (Wwft, Art. 23a; Wwft BES, Art 3.11(1))

(c) Policies and procedures on data protection and information sharing within the group (Wwft, Art. 2f (3); Wwft BES, Art. 1.12(3)). In addition, there are legislative measures in place for FIs to maintain confidentiality relating to UTRs and STRs, including safeguards to prevent tipping-off (Wwft, Art. 23; Wwft BES, Art. 1.5, 3.10).

***Criterion 18.3* –** FIs are required to ensure that their foreign branches and majority-owned subsidiaries in non-EU member states apply AML/CFT measures consistent with the Wwft, if the minimum requirements of the host country are less strict than in the Wwft, insofar as the law in the host country does not prevent it (Wwft, Art. 2(1)). If the law of the host country precludes the application of the Wwft, the FI must inform its supervisor and take measures to control the ML/TF risks (Wwft, Art. 2(2)).

If the foreign branch or majority-owned subsidiary is in another EU member state, the FI must ensure that the branch or subsidiary complies with the provisions in that member state transposing the provisions of AMLD4. However, this does not cover AML/CFT measures in situations where the host country has not adequately implemented AMLD4 or where the rules in the Wwft are stricter than the rules required by AMLD4.

BES Islands: FIs other than MVTS must ensure that their branches and subsidiaries carry out CDD that is equivalent to the measures in Wwft BES, Art. 2.2, and retain records (Wwft BES, Art. 1.6(1)). If the application of these provisions are not permitted in the host country, the FI must notify the supervisory authority and implement measures to mitigate the ML/TF risk (Wwft BES, Art. 1.6(2)). However, this does not include the full range of AML/CFT requirements in the Wwft BES.

Weighting and Conclusion

FIs must have policies, procedures and measures in place, proportionate to their size and these must be applicable at group level. FIs in the Netherlands determine if they need an independent audit function based on their size and complexity. It is not clear how this is consistently applied. There is no requirement for FIs in the BES Islands to screen employees, have an independent audit function or to share UTR information within their groups.

Recommendation 18 is rated largely compliant.

Recommendation 19 – Higher-risk countries

In its last MER, the Netherlands was rated partially compliant with former R.21. There were no specific enforceable obligations for FIs to give special attention to business relationships and transactions with persons from or in countries that do not or insufficiently apply the FATF Recommendations, or to examine the background and purpose of unusual transactions. Existing countermeasures were also found to be limited in scope.

Criterion 19.1 **–** FIs must conduct EDD to business relationships and transactions with natural and legal persons (including FIs) if there is a higher ML/TF risk (Wwft, Art. 2b(2) and 8(1)). FIs must take into account, *inter alia*, countries designated by the EC as a State where an increased risk of ML or TF exists (Wwft, Art. 8(1)(b)), as well as the factors listed in Annex III of the AMLD4 (Wwft, Art. 8(2)). Annex III refers to countries identified by credible sources, such as FATF mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT system (AMLD4, Annex III, Art. 4).

BES Islands: FIs must conduct EDD if there is a higher risk of ML/TF (Wwft BES, Art. 2.10), including for business relationships or transactions when the customer is resident or established in a jurisdiction posing increased risk of ML or TF. EDD must also be applied to business relationships and transactions from countries identified as having no effective AML/CFT systems on the basis of credible sources such as FATF mutual assessments, detailed assessment reports, or published follow-up reports (Rwft BES Annex D, para 3).

Criterion 19.2 **–** In addition to EDD, the Minister of Finance has the authority to issue a regulation that would require FIs to apply countermeasures proportionate to the risk, in line with INR.19 to countries identified in the delegated acts of the EC pursuant to Art. 9 of AMLD4 (Wwft, Art. 9(2)). However, this authority does not extend to jurisdictions called for by the FATF, unless that jurisdiction has also been designated by the EC.

BES Islands: No equivalent provisions exist in the BES Islands.

Criterion 19.3 **–** The FATF public statements (the so-called black and grey lists) are published on the websites of DNB and AFM after each plenary. FIs are informed of the EC's High-Risk Third Country list via the websites of the relevant supervisors (including for the BES).

Weighting and Conclusion

FIs must apply EDD in high risk situations, including for business relationships or transactions when the customer is resident or established in a jurisdiction designated by the EC. The Netherlands has the authority to issue countermeasures independently of any call by the FATF, so long as that jurisdiction has also been designated by the EC.

Recommendation 19 is rated largely compliant.

Technical compliance

Recommendation 20 – Reporting of suspicious transaction

In its last MER, the Netherlands was rated largely compliant with the former R.13 and SR.IV. Deficiencies related to the following: the 14 days period to report a suspicious transaction did not comply with the requirement of prompt reporting; the definition of TF did not include funds related to those who finance terrorism, limiting the scope of the reporting obligation. Since then, the Netherlands has amended the Wwft provisions on UTRs.

The Dutch reporting system is based on UTRs. The FIU-NL receives UTRs from obliged entities. Based on its own analysis, FIU-NL can declare them suspicious and disseminate them to LEAs.

Criterion 20.1 **–** FIs are required to report unusual transactions to the FIU-NL. A transaction must be reported immediately after its unusual nature has become known. FIs shall use objective[67] and subjective indicators to determine the unusual character. The subjective indicator is defined as "a reason to believe that the transaction may be related to ML or TF" (Wwft, Art. 15 and 16; Annex 1 to Wwft Decree 2018). The reference to transactions which "may be related to" ML or TF, is sufficiently broad to cover transactions associated with all proceeds of a criminal activity. A similar obligation exists in BES Islands (Wwft BES, Art. 3.5).

Criterion 20.2 **–** FIs are required to report all unusual transactions where there is a reason to believe that they may be related to ML or TF, including attempted transactions, regardless of the amount (Wwft, Art. 16; Annex 1 to Wwft Decree 2018; Wwft BES, Art. 3.5; Rwft BES, Annex A).

Weighting and Conclusion

All criteria are met.

Recommendation 20 is rated compliant.

Recommendation 21 – Tipping-off and confidentiality

In its last MER, the Netherlands was rated partially compliant with former R.14. Deficiencies included a protection from criminal liability without a good faith requirement; a narrower protection from civil liability; the tipping-off prohibition did not apply to FIs' directors, officers and employees, nor to information in the process of being reported.

Criterion 21.1 **–** Information provided "in good faith" (Wwft, Art. 16 and 17) cannot serve as a basis for a criminal investigation or prosecution for ML/TF against the reporting institution (Wwft, Art. 19(1)). Where there is a "reasonable assumption" to report UTRs and respond to requests for information from the FIU-NL (Wwft, Art. 16 and 17), the reporting institution cannot incur criminal liability for breaches of its duty of confidentiality (Wwft, Art. 19(2); WvSv, Art. 272). Protection from civil liability applies when the information was provided "on the reasonable assumption" that it implements Wwft, Art. 16 and 17 (Wwft, Art. 20(1)). For both criminal and civil liability, this threshold requires that the institution has acted diligently in assessing

[67] Objective indicators include a list of "automatic" criteria (e.g. specific types of transactions above a certain threshold, transactions for the benefit of natural or legal persons residing or established in high-risk countries, etc.).

all facts and circumstances. This threshold is higher than the good faith requirement.[68] This protection extends to employees who made the report or provided information. The legal protection is available even if an institution or employee did not know precisely what the underlying crime was, and regardless of whether an illegal activity actually occurred.

BES Islands: Similar provisions exist in the BES Islands (Wwft BES, Art. 3.8 and 3.9). However, in relation to criminal liability, there is no requirement for the information to have been provided in "good faith" (Wwft BES, Art. 3.8(1)). The protection from violation of the duty of confidentiality is subject to a "reasonable presumption" that the information was provided pursuant to the obligations under Wwft BES, Art. 3.5 or 3.6 (reporting UTRs and responding to requests from FIU-NL). This goes beyond the "good faith" threshold. The protection from criminal liability applies to directors and employees of the FI.

In relation to civil liability, FIs can be held liable if "a plausible case is made that in view of all the facts and circumstances the disclosure should not, in reasonableness, have been made". This requirement is not in line with FATF Standards, as FIs must be protected whenever they report in good faith. Furthermore, there is no specific provision extending the protection to directors or employees (Wwft BES, Art. 3.9).

Criterion 21.2 – FIs and their employees must maintain confidentiality in relation to UTRs and any requests for information received by FIU-NL, or whether the provision of information resulted in an investigation (Wwft, Art. 23). There are specific provisions allowing for consultation and information exchange amongst institutions belonging to the same group, or between these institutions and their branches or subsidiaries (Wwft, Art.23(6); Wwft BES Art.3.11).

BES Islands: Similar provisions exist in the BES Islands (Wwft BES, Art. 3.10 and 3.11). However, the legal obligation does not cover directors or employees of an FI.

Weighting and Conclusion

FIs, their directors and employees are protected from criminal or civil liability when submitting UTRs and other information to FIU-NL. However, this protection is subject to certain offences and narrower conditions than the good faith requirement. Furthermore, the protection from criminal liability in the BES Islands is not limited to cases where the information was provided in good faith and the protection from civil liability does not extend to directors or employees. Tipping-off provisions are in place, but do not explicitly cover directors or employees in the BES Islands.

Recommendation 21 is rated largely compliant.

Recommendation 22 – DNFBPs: Customer due diligence

In its last MER, the Netherlands was rated partially compliant with the requirements of former R.12. Shortcomings related to the scope of the activity subject to CDD measures for real estate agents, and the scope for TCSPs, and some exemptions of CDD requirements for lawyers and notaries.

[68] See also the 3rd round Netherlands MER, p. 178.

AML/CFT legislation for DNFBPs

DNFBPs, except trust offices, are subject to the same CDD requirements within the Wwft as FIs. For trust offices, CDD measures in the Wtt apply (but some Wwft provisions also apply).

DNFBPs, except for trust offices, in the BES Islands are exempt from a requirement to put in place policies, procedures and measures to mitigate and effectively manage and mitigate ML/TF risks. (Wwft BES, 1.13). Articles 2.14-2.19 Wwft BES apply to trust offices in addition to the general requirements. Shortcomings in terms of scope identified in c 22.1 affect all other criterion in R.22.

Criterion 22.1 - DNFBPs in the Netherlands are required to comply with the CDD requirements set out in R.10 in the following situations:

- **a.** Casinos are required to conduct CDD when establishing business relationships or engaging with customers in occasional transactions of more than EUR 2 000 when entering a bet and paying out a prize (Wwft, Art.3(5), 3(7)), and to link the CDD information to transactions made by the customer (Wwft, Art. 3(2)(d)).

  BES Islands: Casinos are required to perform CDD when providing services and performing occasional transactions above USD 3 000 (Wwft BES, Art.1.8 et seq., 2.2(2)(d)).

- **b.** Natural persons, legal entities or partnerships acting as an intermediary with transactions involving the real estate must perform CDD on the customer in a real estate transaction (Wwft, Art.3(2)(a) and (13)).

  BES Islands: There is no requirement for real estate agents involved in a transaction to carry out CDD on both the buyer and seller.

- **c.** DPMS are required to conduct CDD when they perform occasional transactions above EUR 10 000 (in one or more transactions) (Wwft, Art. 3(6)). When acting as intermediaries, DPMS are required to perform CDD when they enter into a business relationship or when conducting an occasional transaction at or above EUR 15 000 (Wwft, Art. 3(5)).

  BES Islands: DPMS are required to carry out CDD when they perform occasional transactions above USD 11 000 (Wwft BES, Art.2.3(1)(b)).

- **d.** When preparing or carrying out activities for their clients in relation to the activities set out in c.22.1(d), lawyers, notaries, other independent legal professionals and accountants are required to comply with the requirements set out in R.10 (Wwft, Art. 3(5)). This equally applies the BES Islands (Wwft BES, Art. 2.13), except when they organise contributions for the creation, operation or management of companies. However, notaries can only refuse to provide services in certain situations, for example, where there is evidence of a sham structure or frontman.

- **e.** TCSPs are required to comply with the requirements in R.10 in relation to the activities set out in c.22.1(e) (Wtt, Art. 22; Wwft, Art. 3(5)). In the BES Islands, providers of business addresses are not covered unless the service is provided in combination with the provision of administrative and advisory services (Wwft BES, Annex A, Art. 1.1).

Criterion 22.2 - DNFBPs must comply with the record-keeping requirements in R.11 (Wtt, Art. 37 for trust offices in the Netherlands; Wwft, Art. 34).

Criterion 22.3 - DNFBPs are required to comply with the PEP requirements set out in R.12 (Wtt, Art. 34 for trust offices). The deficiencies in R.12 apply to DNFBPs.

Criterion 22.4 - DNFBPs in the Netherlands and trust offices in the BES Islands must take adequate measures to prevent the risks of ML/TF resulting from new technologies (see R.15; Wtt, Art. 14)).

Criterion 22.5 - DNFBPs are required to comply with the same reliance on third party requirements for FIs (see R.17). Trust offices are not permitted to rely on third parties for CDD, unless the third party is part of the same group as the trust office (Wtt, Art. 23).

Weighting and conclusion

DNFBPs are required to comply with most of the CDD requirements set out in R.10, 11, 12, 15 and 17. Notaries can only refuse to provide services in limited situations. DNFBPs, except trust offices, in the BES Islands are exempt from a requirement to take measures to manage and mitigate risks. Furthermore, there is no requirement for BES real estate agents involved in a transaction to carry out CDD on both the buyer and seller.

Recommendation 22 is rated largely compliant.

Recommendation 23 – DNFBPs: Other measures

In its last MER, the Netherlands was rated partially compliant with former R.16. Deficiencies noted for FIs also applied to DNFBPs. In addition, TCSPs providing a registered office, business address for a legal entity on a standalone basis were not subject to the reporting requirements, while real estate agents were only required to report one part of the transaction, not both the buyer and seller.

Criterion 23.1 – Most DNFBPs are required to report UTRs to FIU-NL immediately upon identification of suspicion. This applies to conducted and proposed transactions (Wwft, Art.16). Notaries are not able to submit a UTR until a business relationship has been established. Casinos are not subject to UTR requirements when they conduct occasional transactions below EUR 2 000. This is a minor deficiency.

BES Islands: DNFBPs are subject to UTR requirements (Wwft BES, Art. 3.5).

Criterion 23.2 – DNFBPs (see c.22.1) are subject to the same measures as FIs as described in c.18.1 and c.18.2. For trust offices the same measures apply to Wwft-specific requirements (e.g., compliance officer for Wwft-specific requirements). Additionally, trust offices are subject to similar measures in the Wtt for Wtt-specific requirements [Wtt, Art. 15 (audit and compliance function), Art. 67 (training)]. Measures described in c.18.3 also apply to DNFBPs, except for trust offices when the Wtt is applicable (e.g., CDD, EDD and record keeping).

BES Islands: Trust offices are subject to the same requirements as FIs. Other DNFBPs are not subject to the same requirements in c.18.1 and c.18.2, as they are not subject to the requirements in Wwft BES, Art. 1.9 - 1.12 (Wwft BES, Art. 1.13).

Criterion 23.3 - DNFBPs are subject to the same requirements concerning high-risk countries as FIs (Wwft, Art. 8(1); Wtt, Art. 33(1), 36). Therefore, the same deficiencies as identified under R.19 are applicable (see R.19). Deficiencies in c.22.1 on the scope of covered DNFBPs are also applicable. DNFBP supervisors (except for DNB) do not communicate the FATF or EC lists on their webpages.

Criterion 23.4 - DNFBPs are required to comply with the same tipping-off and confidentiality requirements as set out in R.21 (see R.21).

Weighting and conclusion

DNFBPs are required to comply with the requirements of R.20 although casinos and real estate agents in the BES Islands are not required to conduct CDD in all situations and notaries can only submit UTRs once a business relationship has been established. With the exception of trust offices, DNFBPs in the BES Islands are not required to comply with c.18.2 and 18.3. DNB communicates information to trust offices on higher risk countries, while information is not adequately communicated to other DNFBPs.

Recommendation 23 is rated largely compliant.

Recommendation 24 – Transparency and beneficial ownership of legal persons

In its last MER, the Netherlands was rated partially compliant with the former R.33. Deficiencies included the definition of the BO, and issues relating to the issuance of bearer shares.

Criterion 24.1 **–** All companies and other legal persons and companies in the Netherlands must be registered in the company register of the CoC (Hrw, Art. 5)

a) The different types, forms and basic features of these legal persons are set out in several pieces of legislation:

- *Civil law entities with legal personality (limited liability):*
    - Public legal person, Church Communities, Associations, Cooperatives and Mutual Insurance Companies, Public limited liability companies (NVs), Private limited liability companies (BVs), Foundations, Owners' Associations, European Companies, European Cooperative Societies and European Economic Interest Groupings.
- *Legal entities that do not have a legal personality:*
    - Partnerships, General partnerships and Limited partnerships and Shipping Companies.
- *Sole proprietorships.*

b) The process for creating entities is set out in the legislation that describes the different types and forms of legal persons and is supplemented by general civil law articles. Legal entities with legal personality must be established by notarial deed (BW, Art 2.4 and Wna Title V). Legal entities without legal personality are established by contract or notarial deed. The basic and BO information that legal entities are required to register with the Company Registry is set out in Hrw, chapters 2 and 3 and books 2 and 5 of the Civil Code. Requirements for legal persons and other legal entities to keep records of their BOs is set out in Wwft, Art.10. This information is publicly available.

BES Islands: The different types, forms and basic features of legal persons are described in several pieces of legislation, as is the process for creating these entities.

Technical compliance

Legal persons are created by notarial deed and other legal entities can generally be established by contract or notarial deed.

Criterion 24.2 - The Netherlands assesses the ML/TF risk associated with all types of legal persons, although it is not detailed. There is little distinction between different types of legal persons and the risk they pose. The Netherlands have launched various initiatives aimed at identifying and assessing ML/TF risks of legal persons. Following these initiatives and particular features (e.g., less financial and internal controls for most foundations), The Netherlands considers foundations the legal entity posing the highest ML/TF risk. The ML/TF NRAs for the BES Islands do not assess the ML/TF risks associated with the different types of legal persons.

Criterion 24.3 - The different types of legal persons that must register in the company register is set out in Hrw, Arts 5 and 6. The details of basic information that must be included is set out in Hrw, Art. 9. This includes trading names, date of commencement and the party that owns the undertaking. Additional requirements for registration of specific legal persons is included in Hrb, chapters 3 and 4. This includes:

- Address of the registered office: art. 15 Hrb, Art.15),
- List of directors for NV and BV (Hrb, Art, 22.1), for associations, foundations (Hrb, Art. 28),
- basic regulating powers: these are detailed in the statutes which must be communicated to the company register.

The public information on legal persons in the Company Registry can be accessed by any person online, but some information is only available at a cost.

Criterion 24.4 - Legal persons must register the information mentioned in c.24.3 in the company registry and keep it up-to-date (Hrw, Art. 19(1)).

BVs and NVs are the only legal persons that issue shares and must maintain an up-to-date shareholder register at their premises (BW, Art. 2:85 and 2:194; BW BES, Art. 2:109 and 2:209). Cooperatives need to hold an updated list of their members (BW Art. 2:61(d); BW BES, Art. 2:97(d)) and foundations must hold an up-to-date register of all the persons to whom they made a payment of at least 25% of the total payable amount in that year (Bw, Art 2:290). There are no specific obligations for other legal persons.

BES Islands: Private foundations are not required to maintain a register of their members

Criterion 24.5 - Newly created legal persons must file required information in the Company Register within two weeks. There is also a general obligation to update the Company Registry within a week of any change taking place (Hrw, Art. 19 and 20; Hrw BES, Art. 7-8). Legal entities that are required to maintain a register of their shareholders or members must keep the information accurate and up-to-date (see c.24.4). However, there is no mechanism to ensure that these legal entities comply with the obligation to keep the register of their shareholders or members accurate and up-to-date.

Criterion 24.6 - Legal persons and other legal entities incorporated in the Netherlands are required to obtain and hold up-to-date BO information (Wwft, Art.10b). This information (including the nature and extent of the beneficial interest held, and on the identity of the BOs) must be registered in the company register (Hrw, Art. 15a and 19) and applies to all relevant types of legal persons, except:

- listed limited liability companies complete subsidiaries (subject to EU transparency requirements and low risk);
- associations of proprietors (low risk);
- informal associations with no legal personality, rights or obligations and not allowed to own registered goods (such as real estate) (low risk)
- public legal persons (low risk);
- historical legal persons (very rare and low risk);
- sole proprietorship (no legal entity nor legal personality and the only owner is the sole proprietor and thus already known).

Obliged entities must identify the BO of their clients (Wwft, Art. 3(2)(b) Wwft) and cannot solely rely on the BO register (Wwft, Art. 3(15) Wwft). Any discrepancies identified when identifying clients must be reported to the company register (Wwft art. 10(c)).

BES Islands: there are no specific mechanisms to ensure that BO information is obtained by legal persons or other legal entities or available in a specific location, but the tax authorities hold some information (Belastingwet BES, Art. 5(1), (9) (10)). FIs and DNFBPs covered by the Wwft BES are required to collect BO information as part of their CDD procedures (Wwft, 2.2(2)(b)), which can be accessed by competent authorities. However, competent authorities do not have access to data on which FIs or DNFBPs hold the relevant BO information.

Criterion 24.7 - BO information held by legal entities must be accurate and up-to-date (Wwft, Art, 10b (1)). This does not apply to legal entities in the BES Islands, as there is no obligation to hold BO information. Obliged entities must keep BO information up-to-date (Wwft, Art 3(11); Wwft BES, Art, 2.6 (6)).

Criterion 24.8 - The obligation to register basic and BO information to the company register falls on the person who owns the company or each of the directors of the legal person (Hrw, Art. 18(1); Hrw BES, Art. 5-6), which can include a legal representative such as a director. Where this is not possible, the responsibility lies with an individual in the Netherlands with responsibility for the day-to-day management of the legal person (Hrw, Art, 18(2) and (3); Hrw BES, Art, 5(3)). There is no requirement for legal persons and other legal entities to register BO information in the BES Islands.

There is no explicit obligation requiring natural persons resident in the Netherlands to be authorised or accountable to provide basic or BO information directly to competent authorities.

General AML/CFT obligations apply to DNFBPs, including lawyers and notaries (see R.22). There is no explicit requirement for DNFBPs to provide basic and BO information to competent authorities or to give further assistance, but LEAs can subpoena information as part of a criminal investigation and the FIU-NL can request BO information from FIs and DNFBPs (Wwft, Art. 17).

Criterion 24.9 - Obliged entities are required to retain all CDD data in an accessible manner for five years after the date of termination of the business relationship or up to five years after completion of the relevant transaction (Wwft, Art. 33(3); Wwft BES, Art. 2.13). BO information must be retained for a period of 10 years after termination of the registration of the legal entity (Hrb, Art. 51c), except in the BES islands where there is no obligation to obtain BO information.

Criterion 24.10 - Competent authorities, including LEAs, have powers to obtain timely access to the basic and BO information on legal persons. This information can be obtained directly through the company registry. Supervisors, LEAs and FIU-NL can request information directly from obliged entities through their powers.

Criterion 24.11 - The issuance of bearer shares is prohibited since July 2019. Prior to this, NVs were the only legal person that could issue bearer shares. For NVs listed on a regulated market, bearer shares were de-materialised in 2011 requiring holders of bearer shares to change them to regular registered shares at the issuing company, or deposit and register their shares at a central institution or an intermediary.

The issuing NVs were required to change their articles of association to convert bearer shares into registered shares and became the owner of the bearer shares that were not presented or registered by the end of 2020. Holders of (former) bearer shares can still receive their registered shares if they present their former bearer shares to the issuing company before 1 January 2026, but have lost all rights under those shares until presented.

BES Islands: Bearer shares in the BES Islands are prohibited (Bv BES, Art. 104(2)).

Criterion 24.12 - Nominee shareholding and directorships are not a recognised concept in Dutch legislation but professionals offering a nominee-director services are classified as 'trustkantoren', which is a Dutch word similar to TCSP and are licensed under the Wtt (Art. 1.1). Non-professional natural/legal person can also be nominee-director without having to comply with the Wtt obligations. There are also no mechanisms that require nominee directors to disclose the identity of their nominator to the Company Register or to obliged entities. Legal persons are prohibited from providing trust services, unless licensed.

Criterion 24.13 - Sanctions are available for natural and legal persons that fail to comply with the requirements in R.24. However, as noted above, not all requirements are met. There is no obligation to obtain and hold up-to-date BO information and register it in the company register for legal entities incorporated in the BES Islands or other legal entities (e.g. associations, mutual insurance companies, church communities) that are not required to maintain a register of their shareholders or members. Therefore, sanctions are not available for these entities.

It is an economic offense to fail to register with the Company Register basic company and BO information, accurately or in a timely manner (Wed, Art. 1(4)), Art. 6(1)(5); and Hrw, Art. 47). This offense carries a fine of up to EUR 21 750 or imprisonment for up to six months. Existing legal persons have until 27 March 2022 to fulfil this obligation. Newly created entities since 27 September 2020 have to register their BOs immediately.

Public and private limited liability companies are required to maintain the register of shareholders and to keep it up to date (BW, 2:85, 2:194). Art. 2:61(b)(d) for members of cooperatives; 2:290 BW for beneficiaries of foundations). Failure to comply constitutes an economic offence (Wed, Art. 1(4), Art. 6(1)(5); Hrw, Art. 47). This fine is up to EUR 21 750 or imprisonment for up to six months. Legal entities are also required to maintain BO information, and in the process of registering the BOs it is required to provide documentation on the nature and extent of the beneficial interest held for each BO. This applies to nearly all legal entities.

BES Islands: Legal and natural persons are subject to various sanctions for failure to comply with requirements, including a fine of up to USD 28 000 for the criminal act of deliberately submitting a false or incomplete statement to the company register (Hrw BES, Art. 21).

Criterion 24.14 –

a) Basic information in the company registry is publicly accessible online, including for foreign competent authorities. Some information is only available at a cost.

b) Details on BOs, including shareholders, are included in the BO register. This data is also publicly accessible, including for foreign counterparts at a cost.

FIU-NL can also exchange information (including information on shareholders) with foreign counterparts (Wwft, Art. 13b and 16a; Wwft BES, 3.2) or other FIUs (see c.40.9 for deficiencies related to non-EU/EEA FIUs).

BES Islands: Basic information is not publicly available. Supervisors can share basic information with foreign counterparts upon request (see R.40).

c) Competent authorities including the FIU-NL are able to share BO information obtained using investigative powers with foreign counterparts (Wwft, Art. 17 and 22a; Wwft BES Art 3.6). LEAs can also share this information following a request for legal assistance. In such cases, LEAs have the same powers to collect information as they would have in a Dutch investigation into the same offences (Sv, Art. 5.1.8).

Criterion 24.15 - The quality of assistance received from other countries in response to requests for basic and BO information or requests for assistance in locating BOs residing abroad is safeguarded by procedures used by the Central Liaison Office of the Tax and Customs Administration and IRCs.

The Dutch authorities consider the following information in order to monitor the quality of assistance received from other countries:

- type of response from abroad (full or partial response);
- grounds for refusal if information is not provided;
- possible relevance of the information obtained (insofar as the competent authority is able to assess this); and
- completeness and clarity of the response.

Weighting and Conclusion

Information on the establishment of legal persons in the Netherlands is set out in legislation and is publicly available. All legal persons must be registered on the Company Register. A full assessment of ML/TF risks of all legal persons has not been carried out. However, The Netherlands have launched various initiatives aimed at identifying and assessing ML/TF risks of legal persons. Obliged entities are required to keep BO information accurate and up-to-date in a central register, but minor deficiencies exist. Nominee directors and nominee shareholders are subject to AML/CFT obligations in some instances, which somewhat mitigates the overall risk.

Recommendation 24 is rated as largely compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In its last MER, the Netherlands was rated partially compliant with former R.34. Deficiencies related to gaps in the BO definition of legal arrangements, the scope of legal privilege hindering the possibility for LEAs to access BO information regarding trusts held by some DNFBPs, the updating requirement for trust BO information being insufficient to ensure it is accurate, complete and available in a timely manner.

Criterion 25.1 –

(a) Express trusts cannot be established in the Netherlands or in the BES Islands. For "Mutual Funds", which are a similar legal arrangement in the Netherlands, there are no explicit requirements for custodians to obtain and hold adequate, accurate, and current information on the identity of the participants, the administrator or other natural persons exercising ultimate effective control. In some cases, Mutual Funds are investment funds, subjecting them to registration and supervision by the AFM (Wft, Art. 2:65). The Netherlands is party to the Hague Trust Convention[69] which means that foreign trusts as defined in the Convention are recognised. Professional trustees in the Netherlands of such trusts are required to carry out CDD measures on the express trust itself, which include determining the BO (Wtt, Art. 30(3)(a)). In the BES Islands, similar requirements exist, including for the trustee to be aware of the identity of the settlor of the trust and BO of the trust (Wwft BES, Art. 2.18). However, it is not clear if this includes the same identification and verification measures as required for the identity of the BO of the customer. Beneficial owners include the settlor(s), the trustee(s), the protector(s), the beneficiaries, or to the extent that the individual beneficiaries of the trust cannot be determined, the group of persons in whose main interest the trust is set up or operates, and any other natural person who ultimately controls the trust through direct or indirect ownership or by other means (Wwft Decree 2018, Art. 3(e); Bwft BES, Art. 2(d)). However, the definition of beneficiaries of the trust, when those individuals cannot be identified only relate to the group of persons in whose main interest the trust is set up or operates, which is not in line with the FATF Standards.

(b) There is no explicit requirement for custodians to hold basic information on other regulated agents of, and service providers to, the Mutual Fund. Professional trustees in the Netherlands are required to hold and maintain service records on the trust, including for contracts entered into on behalf of the trust (Wtt, Art. 39; Rfm BES, Art. 2.3). However, while this may to some extent cover the necessary basic information, it does not extend to a requirement to always hold and maintain basic information on all service providers to the trust.

(c) Professional trustees of express trusts are subject to the CDD requirements, and required to maintain this information for at least five years after their involvement with the trust ceases (Wtt, Art. 37(4); Wwft BES, Art. 2.19). However, this only extends to trusts as defined by the Hague Convention, and therefore does not cover other similar legal arrangements, including Mutual Funds.

[69] Convention on the law applicable to trusts and on their recognition.

Criterion 25.2 – The CDD information collected by professional trustees is required to be up-to-date (see analysis on c.22.1 and c.10.7(b)). This also applies to service records in the Netherlands (Wtt, Art. 39). Deficiencies noted in c.25.1 also apply.

BES Islands: Trust offices must continuously monitor their clients and the transactions. (Wwft BES, Art. 2:17(d)). Service providers must take reasonable measures to ensure that the data collected as a result of CDD is correct and up-to-date (Wwft BES, Art. 2.2(6)).

Criterion 25.3 – FIs and DNFBPs are required to identify the BO of their customers, including with respect to trusts and to take reasonable measures to verify whether the customer is acting on its own behalf or on behalf of a third party (Wwft Art, 3(2)(f); Wwft BES, Art 2.2(2)(f)). The Wwft does not require trustees to disclose their status. Although the CDD requirements may help ensure that this occurs, this does not translate into an obligation on the trustee to disclose their status as a trustee. There is no equivalent obligation for other types of legal arrangements.

Criterion 25.4 – There are no legal restrictions on trustees providing competent authorities or FIs and DNFBPs with any information relating to trusts, including lawyers or notaries acting as trustees. For professional trustees, DNB is authorised to request any person to provide information (Wtt, 43; Wfm BES, Art.7:8).

Criterion 25.5 – LEAs and FIU-NL have the necessary powers to obtain information held by trustees (and persons in an equivalent position in another type of legal arrangement), and other parties such as FIs and DNFBPs, in the course of their investigations (see R.29, 30, 31). In addition, prosecutors can also require obliged entities to produce information in the case of serious offences (WvSv, Art. 67(1)). Supervisors also have the necessary powers to obtain information on trusts from FIs and DNFBPs (see analysis on R.27, R.28).

Criterion 25.6 – The provisions for co-operation with competent authorities in other countries described under R.37 and R.40 also apply to the exchange of information on trusts and legal arrangements. There is currently no registry that holds basic information on trusts or similar legal arrangements. Foreign competent authorities can access the DNB's public register of licensed trustees, which does not include information on the individual trust or similar legal arrangement. Supervisors can, under certain conditions, provide information obtained in the performance of their tasks, including information collected on CDD, to foreign supervisors, subject to certain safeguards (Wwft, Art. 22a; Wtt, Art. 56; Wwft BES, Art. 1.5(2)). For DNB, this also extends to other foreign government authorities. FIU-NL can exchange information (including information on trusts or other legal arrangements) with FIUs in other EU/EEA member states (Wwft, Art. 13a, 13b and 13c; Wwft BES, Art. 3.2) (see c.40.9 for deficiencies related to non-EU/EEA FIUs).

DNB may, under certain conditions, request information on behalf of foreign supervisory authorities from another country which is a party to a treaty on the exchange of information with the Netherlands (or which is subject to the same binding act of an international organisation as the Netherlands) (Wtt, Art. 45). However, this does not extend to the BES Islands. LEAs can share information following a request for legal assistance, and have the same powers to collect it as they would in a domestic investigation into the same offence (WvSv, Art. 5.1.8).

Criterion 25.7 and 25.8 – Trustees are subject to sanctions for failure to comply with AML/CFT requirements, including for failing to grant competent authorities timely access to information regarding the trust referred to in c.25.1. However, available sanctions in the BES Islands are not fully proportionate and dissuasive (see R.35).

Weighting and conclusion

Express trusts cannot be established in the Netherlands, although persons in the Netherlands can act a trustee for trusts created under the law of other jurisdictions and that foreign trusts can own property or otherwise operate in the Netherlands. Obliged entities involved in the administration of foreign trusts are subject to AML/CFT obligations. Mutual funds can be established and share similar features to trusts. However, these are only subject to registration and supervision where they are considered as investment vehicles. Trustees provided by obliged entities are subject to sanctions, but in the BES Islands these are not proportionate or dissuasive.

Recommendation 25 is rated largely compliant.

Recommendation 26 – Regulation and supervision of financial institutions

In its last MER, the Netherlands was rated largely compliant with former R.23. Deficiencies related to the effective supervision of independent insurance businesses and AFM supervision.

Criterion 26.1 – DNB and AFM are designated to supervise and monitor FIs' compliance with AML/CFT requirements (Wwft, Art 1d(1); Wwft BES, Art 1(1)(p)(1) in conjunction with Article 1(b) Decree on the designation of supervisory authorities).

Criterion 26.2 – Almost all FIs, including Core Principles FIs, MVTS and currency exchanges must be licenced by DNB or AFM before carrying out activities in the Netherlands (Wft Art, 1(a) 4; Wfm BES Art, 1.5(2)). Institutions that provide the services under art 1a (3) (a) are not licensed, but are registered. A physical presence is required for FIs, except for banks registered in other EU Member states providing services to customers in the Netherlands (Wfm Art, 3:15(1)(2); Wfm BES, Art 2:14(j)). Banks must also have a licence from the ECB (Wft Art, 2:11(1)). Shell banks are not permitted in the Netherlands (see c.13.3).

Criterion 26.3 – Supervisors prevent criminals from holding (or being the BO of) a significant or controlling interest, or a management function, in FIs. Legal or natural persons are prohibited from obtaining a qualifying holding in FIs or exercise any control in relation to a qualifying holding in these FIs without a declaration of no objection from DNB, AFM or the ECB (Wft, Art. 3:96; Wfm BES, Art. 3:30). A qualified holding is defined as any direct or indirect holding of at least 10% of the issued share capital or of a comparable holding, or the ability to exercise, directly or indirectly, at least 10% of the voting rights or of comparable control (Wft, Art.1:1; Wfm BES, Art. 3:27 DNB and AFM are required to determine that persons in management functions are fit and proper. This includes consideration of a criminal background (Wfm Art, 3:100; Wft BES, 3:30(1)).

Criterion 26.4 –

a) The Netherland's Financial Sector Assessment Program (FSAP) report was conducted in 2017. Overall, the regulation and supervision of FIs was in line with the core principles. The Netherlands complies with principles of banking, insurance, and securities supervision. This includes the application of consolidated group supervision (Wft, 3.6). The FSAP noted that group supervision significantly improved, but some important powers for comprehensive group supervision were not available.[70]

b) Other FIs are subject to regulation and supervision under the Wwft and Wwft BES, having regard to the ML/TF risks in the sector.

Criterion 26.5 – AML/CFT supervisors must perform their tasks in a risk-based and effective manner, taking account of Article 48 of AMLD4[71] (Wwft Art, 1d(6)). This includes basing the frequency and intensity of AML/CFT supervision of FIs or groups on the ML/TF risks of the obliged entities and the jurisdiction.

BES Islands: The supervisory authority can conduct supervision relating to the services in a risk-oriented manner (Wwft BES, Art. 5.8). There is no requirement relating to frequency or intensity.

Criterion 26.6 – DNB and AFM must periodically review the ML/TF risk profile of obliged entities, including the risks of non-compliance, when there are major events or developments in their management and operations (Wwft, Art.1d(6)) This also applies to financial groups.

BES Islands: There are no specific provisions for when supervisors should review the assessment of risk for FIs.

Weighting and Conclusion

There are minor shortcomings in the application of an RBA, including a lack of process for determining frequency and intensity of supervision. There is no requirement to consider and review the risk in the BES Islands but supervisors can conduct supervision in a risk oriented manner.

Recommendation 26 is rated largely compliant.

Recommendation 27 – Powers of supervisors

In its last MER, the Netherlands was rated largely compliant with former R.29. Deficiencies related to the effective use of sanctions.

Criterion 27.1 **–** DNB and AFM have powers to supervise FIs' compliance with AML/CFT requirements, including in the BES Islands (Wwft, Art. 1d(1); Wwft BES, Art. 5.4 & Art. 1(1)(p)(1) in conjunction with the Decree on the designation of supervisory authorities, Art. 1).

Criterion 27.2 **–** Supervisors are authorised to enter all premises without consent and to require inspection of business information and documents (Awb, Art. 5:15 & 5:17; Wfm BES, Art. 7:7 & 7:10 in conjunction with Wwft BES Art. 5.5(1)).

Criterion 27.3 **–** Supervisors are empowered to compel FIs to provide information without the need for a court order. FIs are required to provide assistance as may reasonably be demanded (Awb, 5:16 & 5:20; Wfm BES, 7:8 in conjunction with Wwft BES Art. 5.5(1)).

Criterion 27.4 **–** Supervisors are authorised to impose sanctions in line with R.35 for failure to comply with AML/CFT requirements. This includes powers to impose a range of disciplinary sanctions, including the power to withdraw, restrict or suspend an FI's license (Wwft Chapter 4, Wft Art1:104(1); Wwft BES, Chapter 5).

---

70 IMF (April 2017) Kingdom of the Netherlands-Netherlands : Financial System Stability Assessment

71 EC Directive (EU) 2015/849

Weighting and Conclusion

All criteria are met.

Recommendation 27 is rated compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

In its last MER, the Netherlands was rated partially compliant with former R.24. Deficiencies related to secrecy issues preventing supervision of lawyers and on effectiveness concerning the monitoring of DPMS, lawyers, accountants and illegally operating casinos.

Criterion 28.1 -

a) Casinos are required to be licensed by the Ksa (Wok, Art. 1(1)(a), 27g(1); Wok BES I, Art. 1).

b) A holder of a permit, the persons determining or co-determining its policy and its BOs must be reliable and suitable (Wok, Art. 4b). Although there are no legal or regulatory measures to prevent the associates of criminals (besides the above-mentioned persons) from holding (or being the BO of) a significant or controlling interest, or from holding a management function or being the operator of a casino, the Netherlands government is the sole shareholder of the only licensed casino. Any privatisation could only be effected by law.

Ksa is the designated supervisor for the only casino in the Netherlands for AML/CFT requirements, and is required to perform its tasks in a risk-based and effective manner (Wwft, Art. 1d(1)(f) & (6)). DNB is the designated supervisory authority for casinos in the BES Islands (Decree on the designation of supervisory authorities under the ML/TF (Prevention) Act BES, Art. 1(b)).

Criterion 28.2 &28.3 - The following institutions are responsible for the supervision of the AML/CFT compliance of the obliged DNFBPs other than casinos:

The Netherlands

- **DNB**: Trust offices (Wwft, Art. 1d(1)(a)).
- **BFT**: Notaries, other legal professionals, accountants and TCSPs acting as a formation agent of legal persons (Wwft, Art. 1d(1)(e)).
- **Deans (NOvA)**: Lawyers (Wwft, Art. 1d(1)(d)).
- **BTWwft**: Real estate agents, DPMS acting as buyers, sellers and intermediaries, and providers of postal addresses that are not covered by the Wtt (Wwft, Art. 1d(1)(e)).

DPMS, when acting as intermediaries, are not supervised for AML/CFT compliance.

The BES Islands

- **DNB**: Trust offices (*Decree on the designation of supervisory authorities under the ML/TF (Prevention) Act BES,* Art. 1(b)).
- **BTWwft**: Real estate agents, DPMS (including when acting as intermediaries), notaries, other independent legal professionals, accountants and (*Decree on the designation of supervisory authorities under the ML/TF (Prevention) Act BES,* Art. 2), lawyers until July 1st 2021.
- **Deans (NOvA)**: Lawyers, as from July 1st 2021 (Wwft BES, Art. 5.4)

Criterion 28.4 -

a) Supervisors have adequate powers to perform their functions, including, *inter alia,* to enter all premises without consent, demand the presentation of or to gain access to all records, documents or information relevant to monitoring compliance, and obliged entities are required to cooperate (Awb, Chapter 5.2; Wfm BES, Chapter 2 Art. 7:7 – 7:10).

b) DNFBPs must ensure that their employees and the executive policymakers are screened, as relevant to the performance of their duties and taking into account the risks, nature and size of the institution (Wwft, Art. 35). Tax advisors, accountant, lawyers, notaries, and real estate agents have to provide their supervisor with a certificate of good conduct when requested (Art. 35a Wwft). Obliged entities from these sectors that register for a trade organisation or professional body are usually required to provide certificate of conduct, which include criminal records checks. However, this does not guarantee that DNFBPs screen whether employees, including senior managers, are criminals or the associate of criminals, as a degree of discretion is allowed in determining what screening procedures are appropriate.

BES Islands: For trust offices, officers who determine or co-determine the policy, and persons entrusted with the supervision of the policy and general course of the operations must be reliable (Wfm BES, Art. 3:4). This includes screening whether the person has been convicted of a relevant crime within the last eight years (Bfm BES, Art. 3:1-3:3).

Lawyers are required to register with the Common Court of Justice of Aruba, Curaçao, Sint Maarten and of Bonaire, St. Eustatius and Saba. Screening measures for lawyers include a requirement of integrity and a clean criminal record in the past 10 years on matters relating to money/financial-economic offences, information/confidentiality issues and integrity. A lawyer cannot be registered without a certificate of conduct.

Notaries must provide a certificate of good conduct for accreditation (Wna BES, Art. 9(c)). Certificates in the BES Islands include the same information as in the Netherlands.

No measures are in place for real estate agents, DPMS, accountants or other legal professionals in the BES Islands.

c) Supervisors have adequate sanctions available for failures to comply with AML/CFT requirements. However, available sanctions in the BES Islands are not fully proportionate and dissuasive (see R.35).

Criterion 28.5 -

a) Supervisors are required to perform their tasks in a risk-based and effective manner, taking into account Article 48(6) to (8) of AMLD4. This requires supervisors, *inter alia,* to base the frequency and intensity of on-site and off-site supervision on the risk profile of obliged entities, and on ML and TF risks in the country (Wwft, Art. 1d(6); Wtt, Art. 41(2)).

Technical compliance

BES Islands: Supervisors may, but are not required to, conduct supervision relating in a risk-oriented manner for all DNFBPs, except casinos (Wwft BES, Art. 5.8).

b) Supervisors are required to take into account the degree of discretion allowed to the obliged entity, and appropriately review the risk assessments underlying this discretion, and the adequacy and implementation of its internal policies, controls and procedures (Wwft, Art. 1d(6); Wtt, Art. 41(2)).

BES Islands: This criterion is not met for DNFBPs, except for trust offices, as they are not subject to requirements to carry out risk assessments or have policies, procedures or controls in place (see c.1.10, c.1.11, c.23.2).

Weighting and Conclusion

Casinos are licensed and DNFBPs covered by the AML/CFT legislation are subject to supervision. Supervisors have adequate powers and sanctions available, however, there are some shortcomings in relation to screening to ensure criminals and their associates are prevented from being accredited or holding a management function or significant or controlling interest, including being a BO in a DNFBP. In addition there are gaps relating to supervision in the BES Islands. Scoping issues mentioned in c.22.1 apply.

Recommendation 28 is rated largely compliant.

Recommendation 29 - Financial intelligence units

In its last MER, the Netherlands was rated partially compliant with former R.26, due to deficiencies related to the incomplete legal framework of FIU-NL and concerns with its operational independence. Other deficiencies related to the access to, and security of, data necessary to fulfil its tasks. In follow-up, the technical deficiencies on operational independence and FIU autonomy were addressed, to be re-rated to largely compliant.

Criterion 29.1 **–** FIU-NL is the national centre for the receipt and analysis of UTRs and other information for the prevention and detection of ML, associated predicate offences and TF, and dissemination of its analysis (including for BES Islands) (Wwft, Art. 12-13, Art. 16; Wwft BES, Art. 3).

Criterion 29.2 **–** FIU-NL is the central agency for the receipt of disclosures filed by all obliged entities. The reporting system is based on UTRs (see R.20). A set of subjective and objective indicators define when a transaction shall be considered unusual, and reported to the FIU-NL immediately after its unusual nature is known (Wwft, Art. 15-16; Wwft BES, Art. 3.5). Indicators include the following:

- A reason to believe that the transaction may be related to ML or TF (Wwft, Art. 15-16; Annex to Wwft Decree 2018; Wwft BES, Art. 3.5, Rwft BES, Annexes);
- Objective indicators related to certain types of operations or thresholds.[72]

[72] The Annex to Wwft Decree 2018 includes a list of indicators for each reporting entity. These include: cash transactions of EUR 10 000 or more, where cash is exchanged into another currency or from small to large denominations; cash deposit of EUR 10 000 or more in favour of a credit or prepaid card; credit or prepaid transactions of EUR 15 000 or more, money-remittances of EUR 2 000 or more; transaction by or for the benefit of a

***Criterion 29.3* –** In addition to UTRs, FIU-NL is able to:

a) Request data or information from an obliged entity that submitted a UTR, or from an institution which, in the opinion of FIU-NL, has data or information relevant to its analysis of a transaction or business relationship (Wwft, Art. 17; Wwft BES, Art. 3.6).

b) Access, directly or indirectly, a wide range of financial, administrative and LEA information to properly undertake its functions. FIU-NL also receives information on cash declarations and disclosures from the Customs (see c.32.6)

***Criterion 29.4* –** FIU-NL conducts:

a) *Operational analysis*: FIU-NL conducts its own analysis to determine whether a transaction shall be declared suspicious. This includes checking information provided in the UTRs, relevant databases, requesting additional information to/from LEAs or obliged entities, or foreign FIUs (Wwft, Art. 13- 14, 17; Wwft BES, Art. 3.2- 3.3, 3.6);

b) *Strategic analysis:* FIU-NL conducts studies of ML and TF trends and typologies (Wwft, Art.13d).

***Criterion 29.5* –** FIU-NL is authorised to disseminate information to LEAs (Wwft, Art. 13 (b), (d), (e) and (f) and Wwft BES, Art. 3.2 (d), (e) and (f)). The dissemination of information is carried out through a secure database accessible to all LEAs.

***Criterion 29.6* –**

a) UTR data is classified as State Secret. FIU disseminations are classified as police secret information governed under the Police Data Act (WPG, Art. 7 and 13.2). Information provided to comply with Wwft obligations is confidential and cannot be used for any purpose other than what is required (Wwft, Art. 22; Wwft BES, Art. 1.5).

b) All staff members working for FIU-NL are enlisted in the Police. They are subject to two screening processes: (1) for their appointment as police officer (General Legal Status (Netherlands Police) Decree, Art. 8); (2) for the security clearance needed as a staff member of the FIU-NL (Police Act 2012, paragraph 3.5.4).

c) A dedicated floor within the building of the Police is governing the physical security in relation to the entry of non-FIU personnel into the premises of FIU-NL. FIU-NL has its own IT system and may make use of the Police facilities (Institutional Decree FIU-NL 2013, Art. 3(6)). Apart from the FIU-NL staff members, only authorised technical staff members of the Police Services Centre with specific clearances are able to gain access to FIU-NL databases, for necessary technical maintenance only.

***Criterion 29.7* –**

a) FIU-NL is an administrative FIU, under the direct governance of the Minister of Justice and Security and housed within the Police. The Minister of Justice and Security is responsible for the overall management, organisation and

natural or legal person residing or established or having its registered office in a state that has been designated as a state with a higher risk of ML or TF by the EC. A similar list of indicators for each reporting entity is in place for the BES Islands (Rwft BES, Annexes).

administration of the FIU. The general management of the FIU has been delegated to the Head of FIU-NL (Institutional Decree FIU-NL, Art. 2(4)). The Head of FIU-NL is appointed, suspended or dismissed by Royal Decree, upon recommendation of the Minister of Justice and Security, in agreement with the Minister of Finance (Wwft, Art.12(3); Wwft BES, Art. 3.1(2))). The Head of the FIU-NL has the responsibility for the decisions to declare an unusual transaction to be suspicious (Institutional Decree FIU-NL 2013, Art. 2(2)).

b) The FIU-NL is able to make arrangements or engage independently with domestic competent authorities or foreign FIUs for obtaining information (Wwft, Art. 13a, 13b, 13c, 17(3); Wwft BES, Art. 3.2). Furthermore, the Head of the FIU-NL has the power to independently and exclusively negotiate on and conclude MoUs and agreements with foreign FIUs or other relevant partners (Institutional Decree FIU-NL 2013, Art. 2(2)(e)).

c) While FIU-NL is located within the Police, it is operationally independent and autonomous. The Head of FIU-NL has full authority of FIU tasks (Institutional Decree FIU-NL 2013, Art. 3 (2)). In addition, employees report to the Head of FIU and the UTR database is only accessible by FIU staff (Institutional Decree FIU-NL 2013, Art. 2 (7) and (8)).

d) The Minister of Justice and Security determines the budget of the FIU-NL in agreement with the Minister of Finance (Wwft, Art. 12(2) and (4); Wwft BES, Art. 3.1(4)). Once the budget is set, the Head of FIU has the authority to decide on the use of financial resources (Institutional Decree FIU-NL 2013, Art. 2(3) and (4)).

Criterion 29.8 – *The* FIU-NL is a founding member of the Egmont Group of FIUs.

Weighting and Conclusion

All criteria are met.

Recommendation 29 is compliant.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its last MER, the Netherlands was rated compliant with the requirements of former R.27.

Criterion 30.1 – Various LEAs are responsible for identifying and investigating ML, TF and predicate offences, including the OM, Police, and special investigation services, including FIOD and KMar.

The *OM* is in charge of criminal investigations and prosecutions and responsible for deciding which cases to pursue (WvSv, Article 132a and 141; RO, Art. 124).

The *Police* has investigators at national, regional and local levels (Police Organisation Decree). The National Unit (LE) and the National Crime Squad (DLR) investigate organised crime, including offences related to ML, TF, and environmental crimes (Police Organisation Decree, Art. 6). Each Police region has competence to investigate TF cases, and deals with other high priority investigations such as those related to human trafficking, fraud, cybercrime and execution of MLA requests (Police Decree, Art. 20-21). For complex cases, the regional police can investigate jointly with, or transfer the case to the DLR and/or the Special investigation services. In addition, there are specialised financial teams active within the Police that carry out their own investigations or provide support to the mixed investigation teams.

The four Special *Investigation Services* conduct investigations on a range of predicate offences, including fraud, ML, trafficking in human being, cybercrime and drug trafficking. The FIOD is in charge of investigating and combating fiscal and financial offences and ML, as well as TF. The other special services include the Intelligence and Investigation Service of the Human Environment and Transport Inspectorate, the Intelligence and Investigation Service of the NVWA and the Investigation Department of the Social Affairs and Employment Inspectorate (Special Investigative Services Act, Art. 2-8).

BES Islands: The designated LEAs to investigate and prosecute ML, TF and predicate offences are the OM BES, the KPCN and RST. The OM BES has a specialised ML public prosecutor. Serious cross-border offences across Aruba, Curacao, St. Maarten and the BES are handled by a Detective Co-operation Team (RST).

Criterion 30.2 – All LEAs mentioned under c 30.1 can pursue parallel financial investigations. Financial investigations are carried out in all criminal investigations where suspicious flows of money and assets are identified, in order to confiscate criminal gains and/or prosecute ML/TF. They are also conducted in all organised offences (Confiscation instruction 2016A009, Ch.4).

For serious offences for which a fine of the fifth category can be imposed, the instrument and procedure of a criminal financial investigation (SFO) may be instituted, independently of the investigation into the predicate offences and in parallel with general financial investigations. SFOs can be initiated during or after the investigation of the predicate offence and can be continued after the predicate offence investigation is closed (WvSv, Art. 126).

BES Islands: A criminal financial investigation is instituted in cases of an offence punishable by a term of imprisonment of four or more years, or an offence that may result in any monetary benefits (including ML offences) (WvSv BES, Art. 177a). Similar to the Netherlands, the OM BES must submit an authorisation to the examining magistrate for the KPCN or specialised services to conduct the investigation.

Criterion 30.3 – All LEAs involved in the investigation of ML, TF and predicate offences are also able to identify, trace and initiate the seizing of assets (WvSv, Art. 141-142).

BES Islands: The KPCN and RST investigate criminal offences and can proceed to confiscation, upon authorisation from OM BES.

Criterion 30.4 – Customs may initiate a financial investigation where they detect an unusual transaction or situation, or upon discovery of a violation in the obligation to declare arising a suspicion of a criminal activity (WvSv, Art. 142; (Tax and Customs Administration) Special Investigating Officer Order 2017, Art. 2). Customs' enquiry aims at identifying and tracing proceeds of crime, terrorist funds or any other assets that may become subject to confiscation, and developing evidence for court proceedings.

The Tax and Customs Administration conducts inspections against tax fraud, with the FIOD conducting financial investigations into ML predicate offences.

BES Islands: BES Customs can initiate a ML/TF investigation where they detect a violation to file a declaration, or if they detect an unusual transaction or situation [BAVPol (Decree on Extraordinary Police Officers) Tax and Customs Administration CN, Art. 2].

Criterion 30.5 – (N/A) In the Netherlands and BES Islands, there are specialised units with powers to investigate ML/TF offences arising from, or related to, corruption offences. The Anti-Corruption Centre within the FIOD may conduct investigations into corruption. The Police Internal Investigation Department has powers for investigating allegations of corruption within the domestic civil service (including in the BES Islands). Within the OM, specialised prosecutors focus on anti-corruption. These anti-corruption units are equipped to also carry out ML/TF investigations and confiscation investigations (including SFOs) in the context of a corruption investigation.

Weighting and Conclusion

All criteria are met.

Recommendation 30 is rated compliant.

Recommendation 31 - Powers of law enforcement and investigative authorities

In its last MER, the Netherlands was rated largely compliant with the requirements of former R.28. The main deficiencies were that the scope of legal privilege hindered the ability of LEAs to locate and trace assets and property. The lack of statistics on investigations also impacted effectiveness.

Criterion 31.1 – LEA powers are set out in the Criminal Procedures Code (WvSv, WvSv BES). The powers can be used in the context of ML, TF and predicate offence investigations. Extended powers can be applied to investigate organised criminal groups suspected to commit serious offences.

a) *Production of records held by FIs, DNFBPs, and other natural or legal persons* – The OM can request and obtain documents and information in case of suspicion of serious offences, including TF, and whenever there is a suspicion of ML (WvSv, Art. 67(1), Art. 96(1), Art. 96a, Art. 126nc, 126nd, 126uc). Data can also be requested from telecommunication providers (WvSv, Art. 126n, 126na, 126nb, 126ng and 126ni). Identification data can be requested and obtained by investigative officers, without prior authorisation (WvSv, Art. 126nc).

In the context of an SFO (see Rec. 30.2), an investigative officer can order any natural and legal person to provide insight into documents or data including information on any assets that belong or have belonged to the subject of the investigation (WvSv, Art. 126a, WvSv BES, Art. 177b).

The Netherlands provided sufficient case-law to demonstrate that legal professional privilege (WvSv, Article 98 and 218) can be waived when letters or other papers are the subject of the offence or instrumental in its commission or when the court considers that the importance of establishing the truth in an individual case outweighs the public interest served by legal professional privilege.

In the BES Islands, the investigating officer may require a person to provide data whenever there is a suspicion of a serious offence allowing for pre-trial detention or if there are signs of a terrorist crime (WvSv BES, Art. 177s). When a SFO is initiated, the investigating officer can request any information and insight into the financial position of the person under investigation (WvSv BES, Art. 177b).

b) *Search of persons and premises* – Regular investigative powers include the power to search persons and places, including premises (WvSv, Art. 55a, Art. 126g(2); Police Act, Art. 7; WvSv BES, Art. 177p). The search of houses/places of residence is subject to a prior authorisation by the OM or the examining magistrate (WvSv, Art. 55a, 96, 96b, 96c, 97, 110, General Act on Entering). The prior authorisation is not required in case of immediate danger.

In the course of a SFO, the OM may request the search of a location or the search of documents and data for the purpose of a seizure (WvSv, Art. 126b and 126c, WvSv BES, Art. 177c).

c) *Taking witness statements* – The examining magistrate, OM and judge may call for witnesses (WvSv Art. 180-191, 210-226, 260(1), 280; WvSv BES, Art. 243-260, 421, 307) upon request or if necessary. Witness statements collected by LEAs may serve as evidence in court (WvSv, Art. 344; WvSv BES, Art. 387, 382).

d) *Seizing and obtaining evidence* – LEAs have power to seize any object which may constitute evidence or demonstrate unlawfully obtained gains (WvSv, Art. 94-119a; WvSv BES, Art. 119, 119a). The special framework under an SFO extends powers to LEAs to obtain documents and other information, or to seize objects without any further authorisation (WvSv, Art. 126 and WvSv BES, Art. 177a).

Criterion 31.2 **–** Police, special investigation services, including FIOD can apply a range of investigative techniques for the investigation of ML, predicate offences and TF, including:

a) *Undercover operations* (WvSv, Art 126h; WvSv BES, Art. 177m). In the Netherlands, these techniques are applicable only to the offences listed in WvSv, Art. 67(1), including all offences with a term of imprisonment of four year or more, as well as to TF and the specific offences listed in Art. 67. As ML offences are encompassed by Art. 67, whenever a suspicion of ML arises during the investigation of any predicate offence, these investigative techniques would be applicable.

b) *Intercepting communications* – upon request from the OM, the examining magistrate can authorise the recording of confidential information, such as conversations and telecommunication in a closed network. With this authorisation the OM can order telephone taps (WvSv, Art. 126l and 126m; WvSv BES, Art. 177o and 177q). Data on telephone traffic can be obtained by the OM without authorisation of the examining judge (WvSv, 126n, WvSv BES, Art.177r) In the Netherlands, these investigative techniques are applicable to the offences listed in Article 67(1) – see analysis above-.

c) *Accessing computer systems* – In the Netherlands, access to computer systems may be obtained in the context of a search of a place (WvSv, Art. 125i and 125j) or once a computer is seized (WvSv, Art. 94). Based on the level of intrusion on privacy, the order shall be given by the OM or the examining magistrate. Upon authorisation from both the OM and the examining magistrate, remote accessing to a computer can be granted (WvSv, Art. 126nba). In BES Islands, there are currently no provisions allowing for access to computer systems.

d) *Controlled delivery* shall be authorised by the Board of Procurators General (WvSv, Art. 126ff(2) and Art. 140a; WvSv BES, Art. 177y(2)).

Criterion 31.3 –

a) LEAs can automatically retrieve information on natural and legal persons holding or controlling a bank account or any other banking products through the Bank Information Referral Portal, if the bank is affiliated to the Portal. Banks in BES are not connected to the portal. In the context of a SFO, the investigative officer can order any person to provide information into the financial position of the individual under investigation (WvSv, Art. 126a, WvSv BES, Art. 177b), without any further authorisation from the examining magistrate.

b) There are measures in place to ensure that the information above can be obtained without prior notification (WvSv, Art.126a (5), Art.126b; WvSv BES, Art.177ka).

Criterion 31.4 – LEAs have access to the police database and other databases in which FIU disseminations are stored (e.g., iCOV). In addition, they can request access to information held by the FIU-NL. The FIU-NL cannot refuse to provide data when the request relates to a serious threat, there is a reasonable suspicion that a person committed an offence, or whenever the request is relates to the prevention or detection of an offence (Bpg, Art. 2:13(2)).

Weighting and Conclusion

LEAs have wide powers to obtain access to all necessary documents and information and a broad range of investigative techniques for their investigations. There are minor shortcomings in relation to the ability to identify in a timely manner whether natural and legal persons hold or control accounts. In the BES Islands, there are currently no provisions to allow for access to computer systems.

Recommendation 31 is rated largely compliant.

Recommendation 32 – Cash Couriers

In its last MER, the Netherlands was rated largely compliant with the requirements of former SR IX. Outstanding deficiencies included the lack of disclosure requirements for transportation by mail or cargo, concerns on the quality of data accessible to FIU-NL and effective use of such information and effectiveness of sanctions.

Criterion 32.1 – Based on EU regulations, the Netherlands applies a declaration system for the transportation of cash and BNI valued at EUR 10 000 or more, entering or leaving the EU (EU Regulation 2018/1672, Art. 3), and a disclosure system for transportation via cargo or mail (EU Regulation 2018/1672, Art. 4). In addition to the EU regulations, the Netherlands imposes a disclosure obligation for all physical transportation of cash, BNI and valuable goods of EUR 10 000 or more (Adw, Art. 3:4

Technical compliance

and 3:5). The disclosure obligation is applicable from the moment of entry via an intra-EU border or via air into the national airspace or by sea in the contiguous zone (Adw interpretive note).

BES Islands: The BES Islands implements a declaration system for the transportation of cash, BNI and valuable goods of USD 10 000 or more (Wwft BES, Art. 1.1h and Art. 4.2) and a disclosure system for transportation via mail or cargo (Wwft BES, Art. 1.1h and 4.3) and transportation of documents that may indicate ML or TF.

Criterion 32.2 **–** Travellers entering and leaving the EU, shall submit a written declaration form for incoming and outgoing transportation of cash and BNI valued EUR 10 000 or more (EU Regulation 2018/1672, Art. 2 and 3) to Customs.

In the BES Islands, travellers carrying cash, BNI and valuable goods of USD 10 000 or more shall submit a written declaration to Customs. (Wwft BES, Art. 4.2, 5.4).

Criterion 32.3 **–** For the situations described under c.32.1 where a disclosure system is used (inter-EU: transportation of cash/BNIs via cargo and mail; intra-EU: physical transportation of cash, BNI and valuable goods of EUR 10 000 or more), a natural person must make a disclosure to Customs upon request. The disclosure obligation is fulfilled only if the information provided is correct and complete (EU Regulation 2018/1672, Art. 4; Adw, Art. 3:4 and 3:5; Wwft BES, Art. 4.3).

Criterion 32.4 **–** Customs are authorised to verify compliance with the obligation to declare/disclose by inspecting persons, their luggage and means of transport (EU Regulation 2018/1672, Art. 5). These powers can be used also in case of discovery of a false declaration/disclosure or a failure to declare/disclose. Customs authorities can conduct "an extensive cash control inquiry", which includes questions related to the origin and intended use of cash/BNI (Extensive Cash Control Inquiry Form). As the failure to declare cash is also a criminal offence (Adw, Part 10.1), customs are authorised to exercise criminal investigative powers (see R.31).

BES Islands: Customs have similar powers as in continental Netherlands, including the right to entry premises, demanding additional information, inspecting identity, information and documents (Wfm BES, Art. 7:7 - 7:10; Wwft BES, Art. 5.5(1-2); DAW BES, Art. 1:3, 2:51, 2.66(2)). The obligation to declare includes an obligation to provide information on the origin of the currency or BNIs and their intended use. As the failure to declare cash or to do so correctly and completely is also a criminal offence (Wwft BES, Art. 6.1(1)(2)), it shall be investigated by the KPCN.

Criterion 32.5**–** A false declaration or disclosure is subject to criminal sanctions. If the offence is committed intentionally, imprisonment of up to four years or a fourth category fine (up to EUR 21 750) could be imposed (Adw, Art. 10:1(6)). The unintentional failure to declare or disclose cash or the failure to do so correctly and completely is subject to a fine of the third category (up to EUR 8 700) (Adw, Art. 10:1(4) and (5)). In both cases, a tax penalty order (FSB) can be imposed directly by the Tax and Customs Administration (AWR, Art. 76 and General Customs Decree, Art. 10:15). The FSB is an out-of-court criminal fine which could replace the imprisonment sanction. As per the Customs internal guidelines, the amount of the FSB is equal to 10% of the total cash, up to a fine of the third category (EUR 8 700) or 30% of the total cash, up to a fine of the 4th category (EUR 21 750) if the violation is committed intentionally.

These sanctions apply for the sole offence of not declaring or disclosing. If there is any suspicion of ML or TF, sanctions for ML or TF would apply.

BES Islands: A failure to comply with the obligation to declare or disclose (including providing correct and complete information) is punishable by imprisonment of up to two years (if intentional) or six months (if unintentional), or a criminal or administrative fine of the fourth category (USD 14 000) (Wwft BES, Art. 6.1, 5.11, 4.2 and 4.3). The criminal fine can be imposed to replace the imprisonment sanction. The fine is equal to 10% or 30% of the total cash, based on whether the violation is committed intentionally, up to a maximum of USD 14 000 (BES Customs Guidelines).

However, the maximum applicable fines are not proportionate or dissuasive.

Criterion 32.6 – Information about declarations, disclosures, and related information gathered by Customs officials, is provided to the FIU-NL (EU Regulation 2018/1672, Art. 9; Adw, Art. 1:33). Customs makes all cash declaration and disclosure details electronically available to FIU-NL within four days via goAML (Agreement on the Co-operation between the Tax and Customs Administration and FIU-NL, Art. 3; Cash Regulations, part 10.07.00, of the Customs Manual for Safety, Health, Economy and the Environment on the cash application).

BES Islands: Customs is required to promptly transmit data from the declaration and disclosure forms and reports on seizure of money to FIU-NL (Wwft BES, Art. 4.4). The data is transmitted to the FIU-NL without delay through goAML (BES Manual on Cash Transport).

Criterion 32.7– The Netherlands has mechanisms in place to ensure adequate co-ordination among relevant authorities (see R.2). Information on cash declarations and disclosures is accessible to the FIU-NL, the AMLC, the Tax and Customs Administration and iCOV. There is also co-operation between Customs and other security staff operating at the airports, to ensure that information on any cash obtained during a security check is notified to Customs. Whenever there is a suspicion of ML or TF, the person/case is transferred to KMar or FIOD, which cooperate with the Customs and the OM in the Cash Cooperative Venture (SVLM).

BES Islands: Customs have exclusive access to information in cash applications, and there is co-operation with the FIU-NL (which receives the declarations) as well as with airport security staff. Security staff will notify Customs if any cash is found during a security check.

Criterion 32.8– Competent authorities are able to temporarily restrain currency or BNIs to ascertain whether there is evidence of ML/TF in cases where (a) there are indications that the cash/BNI is related to criminal activity or (b) where false declaration or false disclosure is made (EU Regulation 2018/1672, Art. 7). Customs have the power to detain cash as long as the person subject to the declaration/disclosure obligation has not provided the information required (Adw, Art. 3:3). Furthermore, Customs have powers to seize and confiscate cash, if there is a suspicion of a criminal offence ("Special Investigating Officer (Tax and Customs Administration) 2017", Art. 2).

BES Islands: Customs can confiscate cash/BNI when the discloser does not immediately provide the information requested for declarations or disclosures, or if there are doubts on the accuracy of information (Wwft BES, Art. 5.5). The same powers apply when there is a suspicion of criminal activities (Wwft BES, Art. 4.2(2) and 4.3(2)).

Criterion 32.9– EU Competent authorities can exchange information on declarations and disclosures with third countries (EU Regulation 2018/1672, Art. 10 and 11).

Technical compliance

Customs record and retain information included in declarations for five to seven years, including declarations/disclosures above the threshold, false declarations/disclosures and where there are suspicion of ML/TF. All documentation acquired, including the declaration form, is retained. Various authorities (FIU-NL, AMLC) can request this information for the purpose of international co-operation. In the BES Islands, cash declaration information are shared with the FIU-NL (Wwft BES, Art. 4.4).

***Criterion 32.10*–** The Netherlands has safeguards in place to ensure that personal data collected meet the GDPR requirements for the processing of personal data, including confidentiality, minimum data processing, and purpose limitation. Customs are also bound by a general obligation of secrecy (EU Regulation 952/2013, Art. 12). Similar provisions are in place in the BES Islands (Wwft BES, Art. 1.5). These measures do not restrict trade payments or the freedom of capital movements.

***Criterion 32.11*–**In the Netherlands (including BES Islands), persons who transport currency or BNI related to ML or TF may be subject to the penalties for false declaration/disclosure (see c.32.5), or to the penalties for ML/TF offences. However, these penalties are not sufficiently proportionate and dissuasive (see also R.3 and 5). Such currency or BNI would be seized as described in R.4.

Weighting and conclusion

The Netherlands has a domestic disclosure system to complement the EU regulation on transportation of cash and BNI. However, there are some minor shortcomings in relation to the proportionality and dissuasiveness of available sanctions (including in the BES Islands).

Recommendation 32 is rated largely compliant.

Recommendation 33 – Statistics

In its last MER, the Netherlands was rated largely compliant with former R 32, due to deficiencies in maintaining accurate and complete statistics.

***Criterion 33.1* –** The Netherlands maintains the following statistics:

- **a)** Number of UTRs received (broken down by sector). However, the total number of FIU disseminations used by LEAs is not recorded, nor those disseminations made by FIU-NL but left unattended. The FIU-NL collects statistics on UTRs and disseminations made available to competent authorities for BES Islands.
- **b)** Number of ML/TF investigations, prosecutions and convictions. However, this information cannot be broken down by the type of ML (e.g., self-laundering, third-party ML) or by predicate offence.
- **c)** Value of seized objects, number and types of seized goods and value of collected confiscations. However, confiscation information cannot be broken down by the type of crime. Furthermore, the Netherlands does not maintain statistics on the value of confiscation orders imposed by the Courts. Statistics on seized and confiscated assets collected in the BES Islands are not comprehensive.

d) Incoming and outgoing MLA requests. However, this cannot be broken down by predicate offenses, and specific MLA statistics for TF are not available (only terrorism statistics are available).

Weighting and Conclusion

The Netherlands maintains statistics in all required fields; however, statistics cannot be disaggregated by predicate offences or type of ML. Statistics on confiscation and MLA, as well as statistics for the BES Islands, are not comprehensive.

Recommendation 33 is rated largely compliant.

Recommendation 34 – Guidance and feedback

In its last MER, the Netherlands was rated partially compliant with former R.25. Deficiencies related to the issued guidance being too general, outdated, incomplete or inaccurate. Feedback from FIU-NL was insufficient.

Criterion 34.1 –

Guidelines and feedback by authorities and supervisors

Most supervisors provide and update guidelines for obliged entities on AML/CFT obligations set out in the Wwft and Sw. Feedback is provided to obliged entities during regular consultations and in the context of public-private partnerships. Guidance is only available to a limited extent in BES Islands.

Guidelines and feedback by FIU-NL

FIU-NL is obliged to provide information on the prevention and detection of ML and TF to business sectors, professional groups, supervisory authorities, the public, and the OM (Wwft, Art. 13(f); Wwft BES, Art. 3.2(f)). Non-confidential information is shared through its website and newsletters and confidential information is distributed through GoAML and newsletters. Relationship managers are appointed by FIU-NL in obliged entities to inform new developments and raise awareness. Public-private sector partnerships with several other banks strengthen the effectiveness of reporting UTRs.

FIU-NL provides a special website, guidance, and feedback for obliged entities in the BES Islands. Local liaisons officers maintain ongoing contact with obliged entities and sector professional bodies.

Weighting and Conclusion

Guidance is available for most sectors and supervisors engage in outreach with obliged entities. FIU-NL provides guidelines and feedback to a large extent, including in the BES Islands. Some guidance is not updated regularly and is limited in the BES Islands.

Recommendation 34 is rated largely compliant.

Recommendation 35 – Sanctions

In its last MER, the Netherlands was rated largely compliant with former R.17. Sanctions were used to a limited degree and fines for large organisations were not dissuasive.

Criterion 35.1 –

R.6 - TFS

Obligations to take administrative and internal control measures to comply with the sanction regulations only apply to FIs and TCSPs. There is no such obligation for other DNFBPs and thus also no sanctions.

Supervisors have different administrative sanctions available for violations of provisions pursuant to rules laid down in accordance with Sw Article 10b, including:

- Instructions to follow a course of action (Sw, Art. 10ba)
- Orders, subject to a penalty (Sw, Art. 10c)
- Administrative fines (Sw, Art. 10d)

The amount of an administrative fine is determined by Order in Council (Sw, Art. 10e). Administrative fines are grouped into three categories for FIs and DNFBPs, where the basic amount vary from EUR 10 000 to EUR 2 000 000, and the maximum amount varies from EUR 10 000 to EUR 4 000 000 (Sw, Art. 10e(2)). In case of repeat offences, the amount of the maximum fine is doubled (Sw, Art. 10e(1)). Supervisors may also impose a gain-based fine, in which an administrative fine can be imposed up to twice the amount of the gain obtained by the offender as a result of the violation (Sw, Art. 10e(3)). Wwft BES, Art. 6.1 and WvSR BES, Art 27 are comparable to the WED as they penalise administrative law standards.

Intentional violations of regulations pursuant to Sw Art. 2, 7 and 9 can be sentenced to a maximum term of imprisonment of six years, community service or a fine in the fifth category for intentional violations, and for violations without intent, detention for a maximum of one year, community service or a fine in the fourth category (WED, Art. 6).

BES Islands: For FIs, failure to comply with sanctions screening measures can lead to imprisonment up to two years or a fine of maximum USD 14 000 or 56 000 for legal entities (Wwft BES, Art.6.1; WvSr BES, Art.27). However, for most DNFBPs there is no obligation for mandatory screening systems or for reporting information to their supervisor. Since there are no such obligations, there is no monitoring and no sanctions available.

R.8 – NPOs

Persons found guilty of TF can be liable to a term of imprisonment not exceeding eight years or a fine of the fifth category (WvSr, Art 421).

There is no NPO supervisor who can impose sanctions for non-compliance with the requirements of R.8. Most NPOs are part of a voluntary sector organisation, which monitors compliance with their self-regulation obligations.

R.9 to 23 - Administrative sanctions (FIs, DNFBPs)

Supervisors have a range of administrative sanctions available to them for violations of provisions in the Wwft, Wtt & Wwft BES, including:

- Instructions to follow a course of action (Wwft, Art. 28; Wtt, Art. 47; Wwft BES, Art. 5.9)
- Orders, subject to a penalty (Wwft, Art. 29; Wtt, Art. 48; Wwft BES, Art. 5.10)
- Administrative fines (Wwft, Art. 30; Wtt, Art. 48; Wwft BES, Art. 5.11)

- Publication of decisions or warnings (Wwft, Art. 32e & 32f; Wtt, Art. 59 & 61; Wwft BES, Art. 5.11 & 5.19)
- Prohibit persons from holding a policy-making position in a FI or DNFBP in the Netherlands (Wwft, Art. 32c; Wtt, Art. 53)
- Revoke, amend or limit a license in a FI or trust office (Wft, Art. 1:104(1)(o) & (q); Wtt, Art. 7(1); Wfm BES, Art. 2.14)

The amount of an administrative fine is determined by Governmental Decree (Wwft, Art. 31; Wtt, Art. 49). Administrative fines are grouped into three categories based primarily on the severity of the violation, where the basic amount ranges from EUR 10 000 to EUR 2 000 000 and the maximum amount ranges from EUR 10 000 to EUR 5 000 000 (Wwft, Art. 31(2-3); Wtt, Art. 49 (2)).

Violations of the most important provisions of the Wwft, Wtt and Wwft BES, are subject to criminal sanctions (WED, Art. 1(1) and (2); Wwft BES, Art. 6(1)). Intentional violations of the Wwft or Wtt can face imprisonment for a maximum term of two years, community service or a fine in the fourth category, which for habitual offences can be increased to a maximum of four years' imprisonment and a fine of the fifth category (WED, Art. 6).

For violations of the Wwft BES, supervisors determine the amount of the administrative fine (Bwft BES, Art. 8(1)). Administrative fines are grouped into four categories ranging from USD 0 to a maximum of USD 500 000 (Bwft BES, Art. 6), which is doubled for violations of the same offence within five years (Bwft BES, Art. 9).

Violations of the Wwft BES are punishable with a term of imprisonment for a maximum of two years or a fine in the fourth category (Wwft BES, Art. 6.1). For violations that are liable to punishment under the WED, the supervisor may either impose an administrative fine or the OM may decide to prosecute. If the conduct subject to an administrative fine is also a criminal offense, it will be submitted to the OM, unless it has been provided by law or agreed with the OM that this may be waived (Awb, Art. 5:44).

Criterion 35.2 –

FIs, DNFBPs

For criminal offences committed by a legal person, measures may be imposed on the legal person and/or on the persons who have ordered the commission of the criminal offence, and the persons who actually directed the unlawful acts (WvSr, Art. 51(1); WvSR BES, Art. 53). This applies to both violations of the WED and administrative sanctions posed by supervisors (Awb, Art. 5:1; Wwft BES, Art. 5.2).

TFS

The WvSR, WvSr BES and Awb is similarly applicable for administrative and criminal sanctions for violations of the Sw or regulations laid down by or pursuant to the Sw.

Weighting and conclusion

The Netherlands has a range or sanctions including license revocation, administrative and criminal sanctions and the publication of warning notices. Administrative and criminal fines apply to FI and DNFBPs and natural persons within obliged entities involved in an ML/TF offence, however, it is unclear in which cases the different type of fines are applied. The levels of administrative fines for violations in the BES Islands are not dissuasive, however, the reputational impact of receiving a fine acts as a deterrent.

Recommendation 35 is rated largely compliant.

Recommendation 36 – International instruments

In its last MER, the Netherlands was rated partially compliant with former R. 35 and SR.I, due to deficiencies in the implementation of the Palermo, Vienna and CFT Conventions and minor shortcomings on the implementation of UNSCRs 1267 and 1373. Further to amendments to its Extradition Act and the introduction of an autonomous TF offence, the Netherlands was re-rated as largely compliant with both recommendations in follow-up.

Criterion 36.1 **–** The Netherlands (including the BES Islands) is party to the Vienna, Palermo, Merida and TF Conventions.

Criterion 36.2 **–** The Netherlands has broadly implemented the provisions of the Vienna, Palermo, Merida and TF Conventions. There are minor deficiencies in relation to the offences of simplified deliberate and culpable self-laundering, which are non-extraditable (see c. 39.1).

Weighting and Conclusion

The Netherlands, including BES Islands, has ratified and broadly implemented the provisions of the Vienna, Palermo, Merida and TF Conventions.

Recommendation 36 is rated largely compliant.

Recommendation 37 - Mutual legal assistance

In its last MER, the Netherlands was rated partially compliant with former R.36 and SR.VI. Deficiencies related to the inability to provide assistance in searching and seizing evidence of ML, for predicate offences other than transnational organised crime or corruption; limitation to the ability to provide MLA due to shortcomings in SR.II, and limitation in the access information and documents held by notaries, lawyers and accountants by LEAs, due to the scope of legal privilege. Further to amendments to the extraditable offences and the introduction of an autonomous TF offence, the Netherlands was re-rated largely compliant with R.36 in the follow-up process.

Criterion 37.1 **–** The Netherlands can provide a wide range of MLA in criminal matters to foreign authorities, including international courts (WvSv, Book 5). Book 5 of WvSv provides the legal basis for international and European legal assistance in criminal matters. Dutch authorities may provide legal assistance to foreign countries regardless of the existence of a treaty or assurance of reciprocity, provided the MLA request is not in breach of national law or goes against the public interest. MLA includes performing or cooperating in investigative activities, establishing the presence of criminally obtained assets, sending documents, dossiers or evidence, providing information, serving documents, providing notices or communications to third parties (WvSv, Art. 5.1.1), search and seizure (WvSv 5.1.8), confiscation (WOTS Art. 13), although certain types of assistance are available only to countries with which NL has a treaty relationship. The Netherlands is party to various multilateral treaties, including the Council of Europe Convention on Mutual Assistance in Criminal Matters and its two additional protocols and the UN Convention against Transnational

Organised Crime. It has also concluded bilateral treaties with, amongst others, the US, Canada, Australia and Hong Kong, China. Judicial co-operation between EU member countries is carried out through European Investigation Orders (EIO) (WvSv, Art. 5.4.1-5.4.31), which are sent directly to the IRCs.

MLA is not conditional upon the existence of a treaty. There are no formal time limits in handling MLA requests. The Ministry of Justice's internal guidelines state that incoming MLAs should be handled within five working days, and outgoing MLAs within three working days. In case a concrete time frame is mentioned in the MLA request, the Department of International Legal Assistance in Criminal Matters (AIRS) shall contact the IRC within reasonable time before the lapse of the time limit, to make sure the request has been executed. If no time frame is stipulated, AIRS contacts the IRC within six months upon receipt of the request. EIOs shall be recognised within 30 days of its receipt. The order must then be executed within 90 days of recognition, with a possibility to extend it by a maximum of 30 days (EU Directive 2014/41, Art. 12).

BES Islands: MLA includes conducting or rendering assistance with investigative acts, forwarding documents, case files or items of evidence, providing information, or serving or delivering documents or giving notices or notifications to third parties (WvSv BES, Arts. 555-560). MLA can be provided to other states without the need for an underlying treaty (WvSv BES, Art. 558). Some international Conventions ratified by the Netherlands also apply to the BES (Council of Europe Convention on Mutual Assistance in Criminal Matters and its First Additional Protocol, Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), as well as the four conventions analysed under Rec. 36). There is no formal time limits in handling MLA requests.

Criterion 37.2 – The Minister of Justice is the central authority for MLA requests, including in the BES Islands. AIRS handles the requests from outside the EU, while IRCs send and receive MLA requests within the EU. ICRs are part of the OM: there are 10 regional IRCs, a national one and a specialised one in serious fraud, environmental crime and asset recovery. The Netherlands uses a national system to register, monitor and track MLA requests (LURIS). IRCs are set up for the purposes of timely prioritisation and execution of MLA requests. AIRS has developed non-official internal guidelines for the assessment and handling of MLA requests in a timely and prioritised manner.

LEAs, including in the BES Islands, deal directly with MLA consisting of requests for information that do not imply the use of coercive means or special investigative powers (WvSv, Art. 5.1.7; WvSv BES, Art. 556).

BES Islands: AIRS will transmit to OM BES any MLA requests coming from outside the EU. EU Requests, including from the Netherlands Caribbean Islands and from continental Netherlands will be directly submitted to IRC Carib. The IRC Carib submits the requests to the IRC OM in Bonaire, who further assigns them to the Police. The IRC Carib is placed under the office of the Attorney General of Curaçao. The IRC Carib uses its own numbering and a manual system to register and monitor MLA requests, and it is not connected to the LURIS system.

Criterion 37.3 – The granting of MLA in both Netherlands and BES Islands is not subject to unreasonable or unduly restrictive conditions. Conditions for refusal includes cases where the request would violate the principle of double jeopardy or conflict with Dutch interests in a criminal prosecution; it would result in a flagrant

Technical compliance

violation of fundamental rights; there are reasons to assume it is connected to a suspect's religious, ideological or political convictions, his nationality, his race or the population group he belongs to (WvSv, Art. 5.1.5 WvSv BES Art.559). For requests not based on a treaty, the principle of dual criminality applies insofar as the investigative powers that can be used to respond to an MLA request are the same envisaged under the Dutch Criminal Code for the same offence (WvSv, Art. 5.1.8; WvSv BES 558.2).

Criterion 37.4 –

a) In general MLA requests cannot be refused on the sole ground that the offense involves fiscal matters. When the execution of the MLA request is of relevance to the State Tax Authorities, an authorisation from the Minister of Justice and Security is required, which must be provided after co-ordination with the Minister of Finance, (WvSv, Art. 5.1.5(7) and WvSv BES, Art. 560.2).

b) There are no grounds for refusal based on secrecy or confidentiality requirements, with the exception of a situation of legal professional privilege. Any investigative results from an EIO cannot be provided, until there is a definite court decision.

Criterion 37.5 – The Netherlands maintains the confidentiality of MLA requests received, and the information contained therein. For the investigative measures where there is an obligation to notify, a so-called "leave procedure" with the court can be followed to withhold the notice in order to protect the confidentiality. (WvSv, Art. 5.1.10(3) and 5.1.11; WvSv BES, Art. 565, Art. 45). For EIO, a standard presumption of confidentiality applies.

Criterion 37.6 – When MLA requests do not involve coercive actions or the use of special investigative powers, dual criminality is not a condition and a wide range of assistance can be given directly by LEAs (WvSv, Art. 5.1.7; WvSv BES, Art. 562).

Criterion 37.7 – Dual criminality is a condition to provide MLA that requires the use of coercive actions or investigative powers (WvSv, Art. 5.1.8). The Supreme Court clarified that it is sufficient that the conduct criminalised in the requesting state can be classified as an offence in the Netherlands. When no identical criminal legal provision exists in the WvSv, the executing Dutch authorities (AIRS, OM, Courts) undertake the necessary efforts to establish double criminality by searching for a legal provision in Dutch law that aims to protect a comparable legal interest, even if it is named differently (Supreme decisions: NJ 1991/359, (paragraph 5.2), HR 30-08-2005, NJ 2005, 541 (paragraph 3.2) and HR 22-09-2009, NJ 2009, 462 (paragraph 3.3.3).

BES Islands: It is sufficient that the conduct criminalised in the requesting state can be classified as an offence in the BES Islands (ECLI:NL:PHR:2016:952 (RO.14, RO.15).

Criterion 37.8 – In the execution of a request for legal assistance from a foreign state, the same investigative powers which could be used in a Dutch investigation into the same offences can be used (WvSv, Art. 5.1.8(1)) (see analysis under R.31).

Weighting and Conclusion

All criteria are met.

Recommendation 37 is rated compliant.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In its last MER, the Netherlands was rated partially compliant with former R.38 due to the shortcoming under SR II, and the scope of the legal privilege for LEAs to access information held by notaries, lawyers and accountants. Furthermore, it was not established that the Netherlands effectively froze and confiscated funds based on a foreign request.

Criterion 38.1 (a-e) – The Netherlands can take action in response to MLA requests from foreign countries based on multilateral or bilateral agreements or an European Freezing or Confiscation Order (EBB) to identify, seize and confiscate property or proceeds from, instrumentalities used in, on intended for use in ML, predicate offenses or TF. The same investigative powers and coercive measures for identification and seizure that could be used in a Dutch investigation can be used in the execution of a request from a foreign state, regardless the existence of a treaty (WvSv, Art. 5.1.8). Authorities can conduct a criminal investigation with parallel financial investigation or an SFO to trace the suspect's assets and identify criminal proceeds and instrumentalities, to the extent that the same investigative powers could be applied to an investigation into the same acts under Dutch law (WOTS, Art. 13). The types of assistance provided in WOTS are available only to countries with which the Netherlands has a treaty relationship. Property (both tangible and intangible, as well as property rights) and property of corresponding value may be seized at the request of a foreign state, if permitted under Dutch law (WvSv, Art. 94(2), 94a(2); WOTS, Art. 13, 13a and 13b). Seizure is only possible if it would also have been applicable for the same offence committed in the Netherlands. On the basis of a treaty request, confiscation orders can be issued based on an irrevocable foreign jurisdiction order (WOTS, Art. 15, 18, 31 and 31a). For non-EU countries, the Netherlands can identify, trace and freeze in response to foreign requests on a treaty basis or regardless of the existence of a treaty relationship (WvSv Art. 5.1.8). However, a request to enforce a confiscation order from a non-EU country can only take place on the basis of a treaty (WOTS, Art. 2). The request to enforce a confiscation order shall be submitted by the OM to the district court within two weeks (WOTS, Art. 18). Within the EU, the Netherlands implements a mutual recognition of freezing and confiscation orders (EU Regulation 2018/1805). These orders are recognised and executed without delay and with the same speed and priority as for a similar domestic case (EU Regulation 2018/1805, Art. 9).

BES Islands: Similar provisions apply to the BES Islands (excluding EU Regulations) (WvSr BES, Art. 35(1)b,c,e; WvSv BES, Art. 579, 579a to 579f, 581, 583, 591 and 591a).

Criterion 38.2 – There is no legal provision allowing the enforcement of foreign non-conviction based confiscation orders, including circumstances where the perpetrator is not available by reason of death, flight, absence or the perpetrator is unknown. However, the authorities provided case law to demonstrate that requests for the tracing of assets, seizure and confiscation under non-conviction based proceedings may be executed as part of MLA co-operation when based on a treaty (WvSv, Art. 5.1.1; WvSv BES, Art. 555; CoE CETS 198, Art. 23(5); ECLI:NL:HR:2013:586).

Criterion 38.3–

a) There are arrangements in place for coordinating seizure and confiscation action with other countries. Netherlands is also a member of the CARIN and ARO networks. The Dutch judicial ARO can be approached by foreign authorities with regard to MLA in the field of confiscation. The OM Carib and IRC CARIB participates in the CARIN/ARIN networks.

b) The Netherlands has a national seizure authority to manage and dispose of property frozen, seized or confiscated. The BES Registrar of the Court of First Instance manages and disposes of seized or confiscated property (Seizure of Confiscated Objects Decree BES, Art. 2).

Criterion 38.4– Confiscated property can be shared with other countries based on bilateral and multilateral agreements, as well as with EU countries (EU Council Framework Decision 2006/783/JHA). Agreements can also be made on a case-by-case basis (including for the BES Islands).

Weighting and Conclusion

There is a system in place to confiscate property laundered, criminal proceeds or instrumentalities. Some limitations exist in relation to the enforcement of confiscation orders outside a treaty or EU framework. There are no legal provisions allowing the enforcement of foreign non-conviction based confiscation orders.

Recommendation 38 is rated largely compliant.

Recommendation 39 – Extradition

In its last MER, the Netherlands was rated partially compliant with former R.39 due to limitation in the extraditable ML offences for non-CoE members, or countries with no extradition treaty; the lack of an obligation to prosecute a suspect domestically where an extradition request is refused purely on the basis of nationality, and the lack of statistics.

Criterion 39.1 – All offences punishable by a custodial sentence of one year or more are extraditable (including BES Islands). While this threshold includes both ML and TF offences, simplified deliberate and culpable self-laundering are not covered. (Uw, Art. 5(1), 5(1)b, 51a, 51a(2); Uw BES, Art. 5(1)a, 5(1)b, 51a, 51a(2)). While there are procedures in place to ensure the timely execution of the requests (Uw, Part B), there are no prioritisation processes. There are no unreasonable or unduly restrictive conditions for the execution of requests (Uw, Art. 9).

Criterion 39.2 – As a general rule, Dutch citizens cannot be extradited, but under certain conditions extradition of Dutch nationals is allowed, even outside the EU framework. Extradition of Dutch nationals is allowed for a criminal investigation and if a guarantee is given that the execution of a possible custodial sentence can take place in the Netherlands and that this sentence may be converted to Dutch standards (Uw, Art.4(2)). A similar rule applies to surrender procedures within the EU. EU countries can no longer refuse to surrender their own nationals, unless they take over the execution of the prison sentence against the wanted person (Council Framework Decision on the European Arrest Warrant). There is no legal obligation to initiate proceedings for the purpose of prosecution of the offenses set forth in the extradition request in case the request is denied purely on the basis of nationality, with the exception of terrorism-related offences (WvSv, Art. 5.3.16). With regard to other offences there is no legal obligation (*aut dedere aut judicare*) to initiate criminal proceedings domestically. This principle also applies in case the extradition is denied on the basis of nationality.

Technical compliance

***Criterion 39.3* –** Extradition requires dual criminality. It is not required that both states use the same terminology, as long as they protect the same legal right in essence. Mere technical differences in law would not pose an impediment to extradition.

***Criterion 39.4* –** Simplified extradition mechanisms are in place. An accelerated procedure allowing for immediate extradition without court proceedings is available when the requested person consents. This procedure can be activated upon a request for provisional arrest. The individual will be extradited within 20 days from his/her consent (Uw, Art. 41- 45, Uw BES, Art. 41-45). Simplified procedures exist within the EU for extradition based on a EAW (European Framework Decision 2002/584/JHA). Extradition in this case does not require the dual criminality test for 32 categories of offenses, including ML/TF (EAW, Art. 2).

Weighting and Conclusion

There is an extradition mechanism in place for ML/TF. Some minor shortcomings remain in relation to the non-extraditable offence of simplified self-laundering and the absence of legal provisions for national proceedings, where the refusal to extradite is based solely on nationality.

Recommendation 39 is rated largely compliant.

Recommendation 40 – Other forms of international co-operation

In its last MER, the Netherlands was rated largely compliant with former R.40, as there was a lack of statistics to assess the effectiveness by LEAs and the broad scope of legal professional secrecy introduced an unduly restrictive condition to exchange information.

***Criterion 40.1* –** Competent authorities are able to cooperate with their foreign counterparts on ML, TF and predicate offences (including in the BES Islands). Authorities cooperate with their foreign counterparts based on international treaties and agreements. Authorities may also provide/receive assistance regardless of the existence of a treaty or assurance of reciprocity, provided the request is not in breach of national law or goes against the public interest (Art. 5.1.4(3) WvSv). Co-operation with EU/EEA counterparts occurs within the EU framework. The Netherlands also engages in international co-operation through its network of liaison officers (including LEAs, OM and Customs), and through participation in multilateral fora, such as Egmont, EUROPOL and INTERPOL. DNFBP supervisors partake in various forms of co-operation. For financial supervisors' international co-operation see c.40.12-c.40.16.

***Criterion 40.2* –**

a) Competent authorities have their own legal basis for providing international co-operation. FIU-NL cooperate with foreign counterparts as outlined under c.40.9. AML/CFT, supervisors cooperate pursuant to Art.27 of the Wwft (see c.40.12). LEAs, OM and Customs cooperate with their foreign counterparts as outlined under c.40.17.

b) There are no impediments for providing and/or requesting co-operation. Nothing prevents authorities from using the most efficient means to cooperate.

c) Competent authorities have clear and secure gateways, mechanisms or channels to facilitate, transmit and execute requests for assistance. The systems are

Technical compliance

protected and access is restricted. For example, FIU-NL has access to the Egmont Secure Web for the exchange of information and to FIU.NET, which is incorporated into EUROPOL. The OM cooperates with its counterparts through a number of platforms, such as EUROJUST. The Police and FIOD use databases and encrypted communication platforms for co-operation.

d) Competent authorities have processes in place to assess and prioritise requests and ensure timely assistance is provided. For example, FIU-NL is required to make use of all its powers and provide information "immediately" to its requesting EU/EEA counterpart (Wwft, Art. 13a(5)). The OM must also ensure the speedy execution of any legal requests it receives (WvSv, Art 5.1.6.). The MLA system provides deadline warnings and a weekly overviews of pending requests. Where supervisory requests are made under multilateral or bilateral mechanisms, all agencies must work within set timeframes.

e) Competent authorities have processes for safeguarding any information received. For example, information received from foreign AML/CFT supervisors (including DNFBP supervisors) (Wwft, Art. 22(a)) may not be used for purposes other than the intended purposes, and may only be transmitted if a number of criteria are met (Wwft, Art.22(2), Art.25; Wwft BES, Art. 1.5). Information received from foreign LEAs are safeguarded and must be treated in line with the WvSv (WvSv, Art.5.1.3; WvSv BES, Art. 557). See c.40.6 for more information.

Criterion 40.3 – Competent authorities have a range of bilateral and multilateral agreements and MOUs to facilitate co-operation with foreign counterparts. Such agreements are not required for Dutch authorities to provide assistance, but can be established promptly if required by foreign authorities. However, a deficiency exists regarding the legal basis for the FIU-NL to cooperate with its foreign non-EU counterparts in the absence of a MoU (see c.40.9).

Criterion 40.4 – Most competent authorities provide feedback in a timely manner to competent authorities, however, this is not systematic and inconsistent across agencies. For example, FIU-NL must provide feedback to its EU counterparts (Wwft, Art. 13a(4-5)). However, there is no explicit provision for FIU-NL to provide timely feedback to non-EU/EEA countries, unless this is stipulated in an MOU. The Netherlands states that FIU-NL may also cooperate with non-EU/EEA FIUs in accordance with Egmont Principles but this is not set out in domestic law (see c.40.9).

Criterion 40.5 –

a) The fact that a request to LEAs involves fiscal matters is not a ground for refusal. Unless provided by an applicable treaty, MLA requests related to tax, duties, customs and exchange criminal offences are subject to an authorisation from the Minister of Justice and Security which can be provided only after co-ordination with the Minister of Finance. (WvSv, Art. 5.1.5(7) and BES WvSv, Art. 560.2). FIU-NL is permitted to exchange information if the definition of an offence of a fiscal nature in a requesting EU or EEA country differs from the definition in Dutch law (Wwft, Art.13a(3)(b)). No restrictions apply to supervisors for the provision of information or assistance of information on the grounds that the request is also considered to involve fiscal matters (Wwft, Art. 22a; Wtt, Art. 56(1); Wft, Art. 1:65; Wwft BES, Art. 1.5(2); Wfm BES, Art. 1.21(a)).

b) There are no financial secrecy laws inhibiting the implementation of AML/CFT measures in the Netherlands (including the BES Islands) (see R.9).

c) Competent authorities may provide assistance even if an investigation or proceeding is underway, unless the provision of assistance could reasonable be considered to impede this investigation or proceeding or would unduly harm the interests of the natural or legal person concerned (Wwft, Art. 13a, 16a; 22(a); Wtt, Art. 56(1); Wft, Art. 1:89; Wwft BES, Art.1:5(2) and Art.1:5(4)(c); Wfm BES, Art. 1.12(a)).

d) There are no restrictions that relate to the type and nature of requesting counterparts (WvSv, Art. 5.1.5, 5.1.7; WvSv BES, Art. 556, 558).

Criterion 40.6 – Competent authorities are prohibited from disclosing confidential information except where necessary or as required by law (Wwft, Art.22; Wtt, Art. 56, Wft, Art. 1:89; Wwft BES, Art.1:5(1)-(2)). The bases for exchanging information also stipulate that information obtained from foreign counterparts can only be forwarded with permission (Wwft, Art.13b(2-3), Art.22a(2), Art.22b(3); Wtt, Art. 56(2-3); Wft, Art. 1:90(2); Wwft BES, Art. 1.5(3-4) WFM BES, Art. 1:21(4-6)). Moreover, in line with the Netherlands' implementation of the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, the use of obtained information or evidence is restricted to the purposes laid down in the request, unless prior consent is given (Wjsg, Art. 39e and f; Police Data Decree, para 5).

Criterion 40.7 – The GDPR, Wpg and the Judicial Criminal Data Act provide rules for the processing of personal data, including the lawfulness of data processing (GDPR, Art.6), and the rights of the data subject (GDPR, Chapter III). Data processing of personal information by FIs and DNFBPs falls under the scope of the GDPR, while data processing of personal information by the FIU and LEAs falls under domestic legislation (Wpg, Art. 17(a); Wjsg, Art.16a). Supervisors must refuse to provide information if the requesting authority cannot sufficiently guarantee the protection of confidential information (Wwft, Art. 22a(2)(d); Wtt, Art. 56(1)(f); Wft, Art. 1:90(1)(d)).

BES Islands: As the GDPR does not extend to the BES Islands, the BES Personal Data Protection Act protects personal information and applies to LEAs. Supervisors must refuse to provide information if the requesting authority cannot protect the information effectively (Wwft BES, Art.1:5(2)(d); Wfm BES, Art. 121(3)).

Criterion 40.8 – Most competent authorities are able to conduct inquiries on behalf of foreign counterparts, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically [Supervisors: Wft, Art.1:51a-e for EU/EEA member states; Wft, Art.1:65 for non-EU/EEA member states; Wwft, Art. 22; Wtt, Art. 56; Wwft BES, Art.1.5; Wfm BES, Art.1:18(2); LEAs: WvSv, Art.5.1.1, 5.1.7 and 5.1.8; FIU-NL: Wwft, 13a(5), for EU/EEA member states only]. However, there is no explicit requirement for FIU-NL to search databases on behalf of FIUs of non-EU/EEA countries.

Exchange of Information between FIUs.

Criterion 40.9 – FIU-NL is required to cooperate with the FIUs of other EU/EEA member states on ML, associated predicate offences and TF (Wwft, Art.13a-b; Wwft BES, Art.3:2(h)). FIU-NL is only required to "maintain contact with foreign government-appointed bodies whose duties are comparable to those of the FIU-NL" (Wwft, Art.13(h)). It is unclear if this requirement covers co-operation with non-EU/EEA countries, as the provisions related to EU/EEA member states explicitly makes reference to AML/CFT co-operation. The Netherlands states that FIU-NL may also cooperate with non-EU/EEA FIUs in accordance with Egmont Principles but this is not prescribed in domestic law.

Criterion 40.10 – There are no legal provisions to prevent FIU-NL from the provision of feedback, upon request or whenever possible, to its EU/EEA FIU counterparts on the use of the information provided by them, as well as on the outcome of the analysis conducted on the basis of such information. While Egmont Principles require FIU's to provide such feedback upon request, there is no relevant requirement in domestic law to provide feedback to non-EU/EEA FIUs (unless articulated in an MOU).

Criterion 40.11 –

(a)-(b) FIU-NL can exchange information (obtained directly or indirectly by FIU-NL), spontaneously or upon request, with another FIU from an EU/EEA member state (Wwft, Art.13, 13a,16(2); Wwft BES, Art. 1:5, 3:2). This includes powers relating to the access of indirect sources (see c.29.3), and information requested from obliged entities (see c.40.8). There is no equivalent legal basis for exchanging relevant information with non-EU/EEA FIUs.

Exchange of information between financial supervisors

Criterion 40.12 – AFM and DNB have a legal basis to cooperate with their foreign counterparts (both EU/EEA and non-EU/EEA) pursuant to a range of provisions on co-operation and exchange of information (Art. 22a(2)(b), Wwft, Art. 22b(1b); 22b(2)(b);Wwft, Art.27; Wft, Art.1.51-2; Wft, Art.1:65; Wwft BES, Art. 1.5(2)(b); Wfm BES, Art. 1:21(3)(b)). If supervision is performed as part of an EU/EEA supervisory college, information is exchanged amongst the established board of supervisors (Wft, Art. 1:54b-1:54c). The Minister of Finance can also exchange information or intelligence obtained during the DNB and AFM's supervision of TFS with foreign counterparts responsible for supervising TFS (including non-EU/EEA authorities) (Sw, Art.10h), but this does not extend to the BES Islands.

Criterion 40.13 – As mentioned in c.40.12, the AFM and DNB can exchange domestically available information, including information held by FIs, in a manner proportionate to their respective needs with their EU/EEA counterparts without additional agreements, and with their non-EU/EEA counterparts in compliance with treaties or agreements on the exchange of information. This is applies to the BES Islands.

Criterion 40.14 –

a) Regulatory information is generally not considered confidential and is therefore available publicly in the Netherlands, including in the BES Islands. Should this type of information be considered confidential (e.g., if individual institutions can be identified), the legal basis for exchange of information described under c.40.12 applies.

b) Prudential supervision is regulated by the Wft (Netherlands) and Wfm BES (BES Islands). The exchange of information as described in 40.12 applies.

c) The DNB and AFM gather AML/CFT information (e.g., internal procedures, policies, CDD information, customer files, samples of accounts and transaction information) in the course of their AML/CFT supervisory activities pursuant to the Wwft and the Wwft BES. The regime for co-operation and exchange of information as described in 40.12 applies.

Criterion 40.15 – The DNB and AFM are authorised to conduct inquiries on behalf of foreign supervisors (both EU/EEA and non-EU/EEA counterparts) relating to their duties as supervisors in the Wft (e.g., for registration and licensing purposes) (Wft, Art.1:52 for EU/EEA supervisors; and Wft, Art.1:68 for their non-EU/EEA counterparts). There are no provisions in the Wwft that allow the AFM or DNB to conduct inquiries on behalf of non-EU/EEA counterparts, and they cannot conduct inquiries themselves in the Netherlands and the BES Islands.

Criterion 40.16 – Supervisors are forbidden from using or disseminating confidential information in any other way than the use for which it was requested (Wwft, Art.22(1); Wft, Art.1:90(2) and 1:93(3)). Supervisors cannot provide information received from foreign supervisors to other domestic or foreign supervisors unless it has received explicit confirmation from the foreign supervisor (Wwft, Art 22b(3) and 22a(3); Wwft. 1.5(3); Wfm BES, Art.1:21(2)).

Exchange of information between law enforcement authorities

Criterion 40.17 – LEAs and OM (including in the BES Islands) can formally exchange information with other LEAs in other countries on the basis of a MLA request (WvSv, Art. 5.1.4; WvSv BES, Art.555). For informal co-operation, information may be exchanged when necessary for a proper execution of a domestic or foreign police task (Police Data Decree, Art.5).

Criterion 40.18 – If an incoming foreign request for information is based on an international treaty, the action will be complied with to the extent possible (WvSv, Art.5.1.4). Requests for MLA outside conventions or agreements may be granted if they are not contrary to a statutory requirement and does not violate public interest (WvSv, 5.1.4(3) and 5.1.5). Requests may include the sharing of information, police data and data from other competent authorities (WvSv, Art.5.1.1). Standard and special investigative techniques can be used in foreign investigations (WvSv, Art.5.1.8). This applies to the BES Islands. For EU co-operation, information and intelligence can be provided by LEAs spontaneously (Police Data Decree, Art.5:3-5:8).

Criterion 40.19 – The OM can establish Joint Investigation Teams (JITs) with foreign counterparts, including non-EU/EEA counterparts (WvSv, Art.5.2.1; Second Additional Protocol ETS 182). There is no legal basis for OM BES to form JITs.

Exchange of information between non-counterparts

Criterion 40.20 – Competent authorities can exchange information indirectly with international non-counterpart authorities provided this is necessary and proportionate [Wwft Art.22a(2)(b) and 22b(2)(b); Wtt, Art. 56(1)(d); Wwft, Art.13a; Wwft BES, Art.3:2. Wwft BES, Art. 1.5(2)(b), Art. 3:2; Wfm BES, Art.12.3(b)].

Weighting and Conclusion

Competent authorities have the powers to provide a wide range of international assistance. There are some limitations in the BES Islands and the lack of an explicit legal basis for FIU-NL to cooperate with non-EU/EEA FIUs in the absence of an MOU.

Recommendation 40 is rated largely compliant.

Technical compliance

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	LC	• The NRAs primarily rely on qualitative inputs, particularly the NRAs of the BES Islands, which may impact the reasonableness of the conclusions on risks. • Some sectors in the BES Islands are exempted from AML/CFT requirements amid the existence of identified risks.
2. National co-operation and co-ordination	C	• All criteria are met.
3. Money laundering offences	LC	• There are minor shortcomings related to the available sanctions for self-laundering and the inability to apply both criminal and civil/administrative sanctions to legal persons.
4. Confiscation and provisional measures	C	• All criteria are met.
5. Terrorist financing offence	LC	• There are minor gaps in relation to the scope of TF offences and the proportionality and dissuasiveness of sanctions.
6. Targeted financial sanctions related to terrorism & TF	LC	• National legislation does not always prescribe in detail how the existing TFS provisions shall be implemented. • There is no obligation for some DNFBPs to communicate the assets frozen or actions taken in compliance with TFS obligations. • Communication of designations or de-listings to FIs and DNFBPs does not always occur immediately.
7. Targeted financial sanctions related to proliferation	LC	• There are some minor shortcomings in relation to the extent of the freezing obligation. • Most DNFBPs have no obligation to implement a screening system or report information to their supervisor and there is no monitoring or sanctioning available.
8. Non-profit organisations	LC	• Outreach initiatives to raise awareness and promote accountability of NPOs are not part of a clear coherent policy. • The supervision does not always focus on the organisations most vulnerable for potential TF abuse and there are few obligations or controls related to the financial situation of NPOs. • Since the TF risk on the BES islands is low, no specific measures are taken towards the NPOs in the BES islands in terms of outreach, supervision, information gathering and investigation.
9. Financial institution secrecy laws	C	• All criteria are met.
10. Customer due diligence	LC	• There is no explicit prohibition on keeping anonymous accounts or accounts in fictitious names, although other measures mitigate this in practice. • There is no requirement for FIs to take into account when previous measures have taken place when applying CDD to existing customers, other than if this took place before the implementation of AMLD4 or the equivalent measures in the Wwft BES.
11. Record keeping	C	• All criteria are met.
12. Politically exposed persons	LC	• There is no strict requirement to have senior management approval for establishing and continuing PEP relationships in the BES Islands. • FIs are required to determine source of assets when establishing or continuing a relationship with PEPs. FIs in the BES Islands are not required to establish the source of funds and there is no express requirement to inform senior management before the payout of life insurance policies.
13. Correspondent banking	PC	• Mandatory EDD measures regarding correspondent banking relationships apply only to respondent institutions outside the EEA.
14. Money or value transfer services	C	• All criteria are met.

Recommendations	Rating	Factor(s) underlying the rating
15. New technologies	PC	• The Netherlands employs a narrow definition of VASPs, which does not cover all activities included in the FATF definition. • The threshold for the application of CDD measures for occasional transactions is higher than the threshold in the FATF Standards. • There is no regime for VASPs in the BES Islands.
16. Wire transfers	LC	• There are no requirements for FIs in the BES Islands to send beneficiary information for batch transfers. • FIs of beneficiaries are not required to have risk-based procedures and measures in place where originator information is regularly not provided.
17. Reliance on third parties	LC	• There is no provision requiring the reliant FI to satisfy itself that third parties are supervised or have measures in place to comply with CDD and record-keeping obligations. • There are deficiencies stemming from the general assumption that all EU member states apply adequate AML/CFT controls.
18. Internal controls and foreign branches and subsidiaries	LC	• FIs determine if they need an independent audit function based on their size and complexity. It is not clear how this is consistently applied. • There is no requirement for FIs in the BES Islands to share UTR information within their groups.
19. Higher-risk countries	LC	• The Netherlands has the authority to issue countermeasures independently of any call by the FATF. However, this only applies where the jurisdiction has been designated by the EC.
20. Reporting of suspicious transaction	C	• All criteria are met.
21. Tipping-off and confidentiality	LC	• Protection from criminal or civil liability is subject to certain offences and narrower conditions than the good faith requirement. • The protection from criminal liability in the BES Islands is not limited to cases where the information was provided in good faith. • The protection from civil liability in the BES Islands does not extend to directors or employees. • Tipping-off provisions in the BES Islands do not explicitly cover directors or employees.
22. DNFBPs: Customer due diligence	LC	• Not all DNFBPs covered by the FATF Standards are required by legislation to comply with the CDD requirements set out in R.10, 11, 12, 15 and 17.
23. DNFBPs: Other measures	LC	• Casinos and real estate agents in the BES Islands are not required to conduct CDD in all situations. • With the exception of trust offices, DNFBPs in the BES Islands are not required to comply with c.18.2 and 18.3. • Information on higher risk countries is not adequately communicated to DNFBPs, other than trust offices.
24. Transparency and beneficial ownership of legal persons	LC	• A full assessment of ML/TF risks of all legal persons has not been carried out. • The concept of nominee shareholdings and directorships are not recognised in Dutch law, but in practice both services can be provided and are not subject to AML/CFT obligations.
25. Transparency and beneficial ownership of legal arrangements	LC	• Mutual funds can be established and share similar features to trusts. However, these are only subject to registration and supervision where they are considered as investment vehicles. Trustees provided by obliged entities are subject to sanctions, but in the BES Islands these are not proportionate or dissuasive.
26. Regulation and supervision of financial institutions	LC	• There are minor shortcomings in the application of an RBA, including a lack of process for determining frequency and intensity of supervision. • There is no requirement to consider and review FIs AML/CFT risk in the BES Islands.
27. Powers of supervisors	C	• All criteria are met.
28. Regulation and supervision of DNFBPs	LC	• DPMS in the BES Islands are not subject to supervision when acting as intermediaries. • There are some shortcomings in relation to screening to ensure criminals and their associates are prevented from being accredited or holding a management function or significant or controlling interest, including being a BO in a DNFBP.

Recommendations	Rating	Factor(s) underlying the rating
		• There are gaps relating to supervision in the BES Islands. Scoping issues mentioned in c.22.1 apply.
29. Financial intelligence units	C	• All criteria met.
30. Responsibilities of law enforcement and investigative authorities	C	• All criteria are met.
31. Powers of law enforcement and investigative authorities	LC	• There are minor shortcomings in relation to the ability to identify in a timely manner whether natural and legal persons hold or control accounts. • In the BES Islands, there are currently no provisions to allow for access to computer systems.
32. Cash couriers	LC	• There are minor shortcomings in relation to the proportionality and dissuasiveness of available sanctions (including in the BES Islands).
33. Statistics	LC	• Statistics cannot be disaggregated by predicate offences or type of ML. • Statistics on confiscation and MLA, as well as statistics for the BES Islands, are not comprehensive.
34. Guidance and feedback	LC	• Some guidance is not updated regularly and is limited in the BES Islands.
35. Sanctions	LC	• Administrative and criminal fines apply to FI and DNFBPs and natural persons within obliged entities involved in an ML/TF offence, however, it is unclear in which cases the different type of fines are applied. • The levels of administrative fines for violations in the BES Islands are not dissuasive.
36. International instruments	LC	• There are minor shortcomings in the non-extraditable nature of the offences of simplified deliberate and culpable self-laundering.
37. Mutual legal assistance	C	• All criteria are met.
38. Mutual legal assistance: freezing and confiscation	LC	• Some limitations exist in relation to the enforcement of confiscation orders outside a treaty or EU framework. • There are no legal provisions allowing the enforcement of foreign non-conviction based confiscation orders.
39. Extradition	LC	• Some minor shortcomings remain in relation to the non-extraditable offence of simplified self-laundering • There are no legal provisions for national proceedings, where the refusal to extradite is based solely on nationality.
40. Other forms of international co-operation	LC	• There are some limitations in the BES Islands and the lack of an explicit legal basis for FIU-NL to cooperate with non-EU/EEA FIUs in the absence of an MOU.

Glossary of Acronyms[73]

	DEFINITION
AFM	Dutch Authority for the Financial Markets
AIRS	Department of International Legal Assistance in Criminal Matters
AIVD	General Intelligence and Security Service
Advw	Advocates Act
Adw	General Customs Act
AMLC	Anti-Money Laundering Centre
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
AMLD	European Anti-Money Laundering Directive
AMO	Asset Management Office
ARO	Asset Recovery Office
ATM	Actualisatie Toezicht Methodologie
Awb	General Administrative Law Act
Bbiv BES	Decree on the safekeeping of seized objects BES
BEH	Economic Enforcement Office of the Tax Office
BES	The islands of Bonaire, St. Eustatius and Saba
BFT	Financial Supervision Office
BO	Beneficial owner
BODs	Special Investigative Services
Bpg	Police Data Decree
BtWwft	Tax and Customs Administration AML/CFT Supervision Office
Bv	Private limited company
BVO Protocol	Protocol for instituting and discontinuing anti-terrorist asset freezing measures
BW	Civil Code
Bwft BES	BES Money Laundering and Terrorist Financing (Prevention) Decree
CARIN	Camden Asset Recovery Inter-Agency Network
CBF	Netherlands Fundraising Regulator
CBS	Statistics Netherlands
CDD	Customer due diligence
CIS	European Customs Information System
CJIB	Central Judicial Collection Agency
CoC	Chamber of Commerce
CoE	Council of Europe
CT	Counter-terrorism
DLR	National Crime Squad of the Police
DNB	Dutch Central Bank
DRZ	An agency of the Ministry of Finance, manages seized and confiscated goods
DTN	Terrorist Threat Assessments
EAW	European Arrest Warrant
EBB	European Freezing or Confiscation Order

73 Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

EC	European Commission
ECB	European Central Bank
EDD	Enhanced due diligence
EIO	European Investigation Orders
FEC	Financial Expertise Centre
FEC TFTF	FEC Terrorist Financing Task Force
FIOD	Fiscal Intelligence and Investigation Service
FIU-NL	Financial Intelligence Unit of the Kingdom of the Netherlands
FP	Specialist Office of the National Prosecution Service
GDPR	European General Data Protection Regulation
Hrb	Commercial Register Decree
Hrw	Commercial register Act 2007
Hrw BES	Commercial register Act for the BES Islands
HSC	Human Security Collective
iCOV	Information Exchange on Criminal and Unexplained Wealth
IRC	International Legal Assistance Centre
IRC Carib	International Legal Assistance Centre for the BES Islands
JITs	Joint Investigation Teams
KMar	Royal Netherlands Marechaussee
KPCN	Dutch Caribbean Police Force
Ksa	Netherlands Gambling Authority
LBA	National Authority for Seized Goods
LCA	National Confiscation Coordinator within the OM
LE	National unit of the Police
LEAs	Law enforcement authorities
LIEC	National Information and Expertise Centre
LIRC	National International Legal Assistance Centre
LBA	National Seizure Authority
LP	National Office of the Public Prosecution Service
MFA	Minister of Foreign Affairs
MIT	Multidisciplinary Intervention Team
NCTV	National Coordinator for Security and Counterterrorism
NOvA	Netherlands Bar
NV	Public limited company
OM	Public prosecution office
OM BES	Public prosecution office of the BES Islands
OM Carib	Public Prosecution Service of Curaçao, St Maarten and Bonaire, St Eustatius and Saba
Rfm	Financial Markets Regulation
Rfm BES	Financial Markets Regulation BES
RST	Detective Co-operation Team across the Netherlands, Aruba, Curacao, St. Maarten and the BES.
SDD	Simplified due diligence
SFO	A criminal financial investigation for serious offences
SNRA	European Supranational Risk Assessment
ST	Steering Team for ML investigations
Sw	Sanctions Act 1977
UTR	Unusual transaction report
Uw	Extradition Act
Uw BES	BES Extradition Act
Wab	Accountancy Profession Act
WED	Economic Offences Act
Wfm	Financial Markets Act

Wfm BES	Financial Markets Act for Bonaire, Sint Eustatius and Saba
Wft	Financial Supervision Act
Wiv 2017	Intelligence and Security Service Act 2017
Wjsg	Judicial Records and Certificates of Good Conduct Act
Wna	Civil-law Notaries Act
WODC	Research and Documentation Centre
Wok	Betting and Gaming Act
Wok BES	Betting and Gaming Act BES
Wpg	Police Data Act
Wtt	Trust and Company Service Providers Supervision Act 2018
WvSr	Dutch Penal Code
WvSr BES	Dutch Penal Code for Bonaire, Sint Eustatius and Saba
WvSv	Dutch Code of Criminal Procedure
WvSv BES	BES Code of Criminal Procedure
Wwft	Money Laundering and Terrorist Financing Prevention Act
Wwft BES	Money Laundering and Terrorist Financing Prevention Act for Bonaire, Sint Eustatius and Saba

www.fatf-gafi.org

August 2022

Anti-money laundering and counter-terrorist financing measures - The Netherlands

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in the Netherlands as at the time of the on-site visit from 27 October to 18 November 2021.

The report analyses the level of effectiveness of the Netherlands' AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.