FATF

2ND FOLLOW-UP REPORT

Mutual Evaluation of the Netherlands

February 2014

FINANCIAL ACTION TASK FORCE

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 (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

CONTENTS

ACRONYMS

AFM	*Autoriteit Financiële Markten* (Netherlands' Authority for financial markets)
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
BFT	*Bureau Financieel Toezicht* (Bureau Financial Supervision)
BTW	*WWFT* Supervisory Bureau
CDD	Customer due diligence
DNB	*De Nederlandse Bank* (the prudential and integrity supervisor for banks and other financial institutions)
DNFBPs	Designated non-financial businesses or professions
FIs	Financial institutions
FIU	Financial intelligence unit
LC	Largely compliant
LEA	Law enforcement agencies
MER	Mutual evaluation report
ML	Money laundering
MLA	Mutual legal assistance
MoF	Ministry of Finance
NC	Non-compliant
OEM	Other enforceable means
PC	Partially compliant
PEPs	Politically exposed persons
R	Recommendation
SR	Special Recommendation
STR	Suspicious transaction report
TF	Terrorist financing
WWTF	*Wet ter voorkoming van witwassen en financieren van terrorisme (*Money Laundering and Terrorist Financing Prevention Act)

MUTUAL EVALUATION OF THE NETHERLANDS: SECOND FOLLOW-UP REPORT

Application to move from regular follow-up

Note by the Secretariat

I. INTRODUCTION

The third mutual evaluation report (MER) of the Netherlands was adopted on 25 February 2011, and the country was placed in a regular follow-up process[1]. The Netherlands reported back to the FATF in February 2013 (first follow-up report). In October 2013, the Netherlands confirmed that it would report to the Plenary in February 2014 (interim report) concerning the additional steps taken to address the deficiencies identified in the report and apply to be removed from regular follow-up at that time.

This paper is drafted in accordance with the procedure for removal from the regular follow-up, as agreed by the FATF Plenary in October 2008 and subsequently amended[2]. It contains a detailed description and analysis of the actions taken by the Netherlands in respect of the core and key Recommendations rated partially compliant (PC) in the MER (none of the core and key Recommendations were rated non-compliant (NC)) and for information, in annex, an overview of the actions taken in relation to the other Recommendations rated PC or NC in the MER based on a detailed report by the Netherlands. The procedure requires that a country "*has taken sufficient action to be considered for removal from the process – To have taken sufficient action in the opinion of the Plenary, it is necessary that the country has an effective AML/CFT system in force, under which the country has implemented the core[3] and key[4] Recommendations at a level essentially equivalent to a Compliant (C) or Largely Compliant (LC), taking into consideration that there would be no re-rating*"[5]. The Netherlands was rated PC or NC on the following Recommendations:

Core Recommendation rated NC (no core Recommendations were rated NC):
R.5 (PC), SR.II (PC)
Key Recommendations rated PC (no key Recommendations were rated NC):
R26 (PC), R.35 (PC), R.36 (PC), SR.I (PC), SR.V (PC)

1 www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationreportofthenetherlands.html

2 Third Round of AML/CFT Evaluations Processes and Procedures, par. 41 www.fatf-gafi.org/media/fatf/documents/process%20and%20procedures.pdf.

3 The core Recommendations as defined in the FATF procedures are R.1, SR.II, R.5, R.10, R.13 and SR.IV.

4 The key Recommendations are R.3, R.4, R.26, R.23, R.35, R.36, R.40, SR.I, SR.III, and SR.V.

5 FATF Processes and Procedures par. 39 (c).

Other Recommendations rated PC
R.6, R.12, R.14, R.15, R.16, R.21, R.22, R.24, R.25, R.33, R.34, R.38, R.39
Other Recommendations rated NC
R.9

As prescribed by the Mutual Evaluation procedures, the Netherlands provided the Secretariat with a full report on its progress. The Secretariat has drafted a detailed analysis of the progress made for Recommendations 5, 26, 35 and 36, and Special Recommendations I, II and V (see rating above). A draft analysis was provided to the Netherlands (with a list of additional questions) for its review, and responses were received. The final report was drafted taking the Netherlands' comments into account. During the process, the Netherlands provided the Secretariat with all information requested.

As a general note on all applications for removal from regular follow-up: the procedure is described as a *paper-based desk review* and by its nature is less detailed and thorough than a MER. The analysis focuses on the core and key Recommendations that were rated PC/NC, which means that only part of the AML/CFT system is reviewed. Such analysis essentially consists of looking into the main laws, regulations and other material to verify the technical compliance of domestic legislation with the FATF standards. In assessing whether sufficient progress had been made, effectiveness is taken into account to the extent possible in a paper-based desk review and primarily through a consideration of data provided by the country. It is also important to note that these conclusions do not prejudge the results of future assessments, as they are based on information which was not verified through an on-site process and was not, in every case, as comprehensive as would exist during a mutual evaluation.

II. MAIN CONCLUSIONS AND RECOMMENDATIONS TO THE PLENARY

CORE RECOMMENDATIONS

Since the 2011 mutual evaluation, the Netherlands has amended its preventive AML/CFT legislation and issued and further updated guidance documents with the aim to address shortcomings identified in the MER with regard to R5. The majority of the shortcomings, including those on beneficial ownership requirements, have now been (largely) addressed. The Netherlands' current level of compliance with R5 is therefore assessed to have reached a level of compliance essentially equivalent to LC.

For SRII, the Netherlands made important progress by criminalising terrorist financing (TF) as an autonomous offence. This legal action fully addresses three of the four technical deficiencies while the fourth deficiency is largely addressed. As a result, the Netherlands' current level of compliance with SRII is essentially equivalent to LC.

KEY RECOMMENDATIONS

For R26-35-36-SRI-SRV, the Netherlands has made sufficient progress in addressing the deficiencies identified in the MER, such that its overall level of compliance can be assessed at a level essentially equivalent to LC.

CONCLUSIONS

Overall, the Netherlands has reached a satisfactory level of compliance with all of the core and key Recommendations.

The mutual evaluation follow-up procedures indicate that, for a country to have taken sufficient action to be considered for removal from the process, it must have an effective AML/CFT system in force, under which it has implemented all core and key Recommendations at a level essentially equivalent to C or LC, taking into account that there would be no re-rating.

The Netherlands has made sufficient progress for all core and key Recommendations. Consequently, it is recommended that the Netherlands is removed from the regular follow-up process.

III. OVERVIEW OF THE NETHERLANDS' PROGRESS

A. OVERVIEW OF THE MAIN CHANGES SINCE THE ADOPTION OF THE MER

Since the adoption of the 2011 MER, the Netherlands focused on strengthening its preventive AML/CFT legislative framework through the adoption of amendments to the Money Laundering and Terrorist Financing Prevention Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*,—the *WWFT*. The amendments entered into force on 1 January 2013. The Netherlands' Ministry of Finance (MoF) and supervisory authorities also issued and recently (January 2014) further updated a related set of guidance papers with the aim to assist institutions[6] with the implementation of the Act. The legislation is supported by a National Threat Assessment which was carried out in 2011 and which is currently being complemented.

The Netherlands also amended its *Criminal Code* to introduce an autonomous TF offence. The amendment to the *Criminal Code* came into force on 1 September 2013.

In response to the Financial Intelligence Unit's (FIU) shortcomings identified in the 2011 MER, the Netherlands strengthened the legal framework of the FIU-NL through amendments to the *WWFT* and issued implementing Decrees and regulations to ensure the FIU-NL's operational independence and simplify its governance model. The Netherlands also took various other initiatives with the aim to improve the functioning of the FIU-NL, as set out in section V below.

Finally, it is relevant to mention the political commitment of the Netherlands' government set out in the *"coalition agreement"*[7] issued when the current government took office in November 2012. This

[6] Art.1(a) gives an overview of which entities/persons qualify as an institution. This overview includes all categories of financial institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) as defined in the FATF's Glossary.

[7] A translation of the government's *"coalition agreement"* can be found via the following link: www.government.nl/government/coalition-agreement. In Dutch politics, a *"coalition agreement"* is an essential and *de facto* binding document highlighting the main policy priorities of a new government.

"coalition agreement" specifically refers to the importance of strengthening the Netherlands' AML/CFT regime to combat ML and TF.

B. THE LEGAL AND REGULATORY FRAMEWORK

Since the adoption of the MER in 2011, the Netherlands has completed key AML/CFT legislative steps:

- The amendment of the *WWFT* came into force on 1 January 2013. The amendment aims to deal with some of the shortcomings identified in the MER, especially in relation to the following preventive measures and the FIU:
  a) a range of CDD requirements;
  b) the suspicous transaction reporting requirement;
  c) the protection from criminal and civil liability for entities filing suspicious transaction reports (STRs);
  d) the exchange of information between supervisors; and
  e) the legal framework for the FIU.
- The amendment to the *Criminal Code* came into force on 1 September 2013 and introduces an autonomous TF offence which addresses most but not all of the shortcomings identified in the MER.

The four statutory AML/CFT supervisors (the Nederlandsche Bank – DNB, the prudential and integrity supervisor for banks and other financial institutions (FIs); the Netherlands' Authority for financial markets – AFM, which supervises the conduct of the entire financial market sector: savings, investment, insurance and loans; the Dutch Tax and Customs Administration, *WWFT* Supervisory Bureau – BTW, responsible for AML/CFT supervision of dealers in goods with high value; and the Bureau Financial Supervision – BFT, which is responsible for AML/CFT supervision for lawyers, civil-law notaries, independent legal advisers, public chartered accountants, public accountant-business administration consultants, tax advisors, civil-law notaries, court bailiffs, and other independent finance economic advisers) issued and further updated guidance material with the aim to assist reporting entities with their implementation of the amended *WWFT* and the Sanctions Act (for implementation of some SRII and SRIII requirements). In addition, the Dutch Ministry of Finance (MoF) issued general guidance for all institutions subject to the *WWFT*. It should be noted that the various guidance papers are not mandatory and, as a result, do not qualify as Other Enforceable Means (OEM). This report only refers to the guidance papers issued by the MoF and the DNB because these are most detailed and relevant for the implementation of the R5 provisions, as discussed below.

IV. REVIEW OF THE MEASURES TAKEN IN RELATION TO THE CORE RECOMMENDATIONS

RECOMMENDATION 5 – RATED PC

To improve the level of compliance with R5, the Netherlands has amended the *WWFT* and issued and recently (January 2014) further updated various guidance papers as described in section III above. The main CDD requirements are provided in the amended Art.3 of the *WWFT* and are set out below.

The amended Art.3(1) provides that an *institution*[8] is required to conduct CDD to prevent money laundering and terrorist financing. Art.3(2) sets out the actions the institution needs to take when conducting CDD:

a. establish and verify the identity of the *customer*[9];

b. identify the customer's *ultimate beneficial owner* [10] and implement adequate risk-based measures to verify the ultimate beneficial owner's identity and, when the client is a legal person, to implement adequate risk-based measures to understand the customer's ownership and control structure;

c. establish the objective and intended nature of the business relationship;

d. conduct continuous monitoring of the business relationship and the transactions carried out during the existence of this relationship to ensure that these are consistent with the knowledge the institution has of the customer and the customer's risk profile and, where relevant, examine the source of the assets used for the business relationship or the transaction;

e. establish that the natural person who represents the customer is authorised to do so;

f. implement adequate risk-based measures to verify whether the customer is acting on his/her own behalf or for a third party;

g. as the occasion arises, establish and verify the identity of the natural person referred to in (e).

---

8 See definition in footnote 6 above.

9 Art.1(b) defines the customer as "the person with whom a business relationship is established or on whose behalf a transaction is carried out." It should be noted that the original version of the *WWFT* in Dutch makes a distinction between natural and legal persons in the definition of the customer. The Explanatory Memorandum to the *WWFT* confirms that the term customer covers both natural and legal persons. In addition, the DNB and MoF guidance documents explain both in the original text and the translation into English that the customer refers to a natural or a legal person. The guidance documents also refer to legal arrangements as a category of customers and use the term legal entities to encompass both legal persons and arrangements. The MoF guidance refers to the registration obligations in the Commercial Registers Act to further define legal entities. The relevant definitions are consistent with the FATF Glossary.

10 Art.1(f) defines the *ultimate beneficial owner* as: the natural person who: 1°holds a share of more than 25% in the issued capital of a customer; 2°can exercise more than 25% of the voting rights at the general meeting of shareholders of a client; 3°can exercise actual control over a customer; 4°is the beneficiary of 25% or more of the assets of a customer or trust; or 5° has special control over 25% or more of the assets of a customer, unless the customer is a company subjected to disclosure requirements as referred to in EU Directive 2004/109/EC (publicly listed companies).

Art.3(3) contains the CDD measures which an institution is required to take when the customer is acting as a trustee. The institution shall take adequate risk-based measures to understand the trust's ownership and control structure and shall, for this purpose:

a. identify the trust's settlors and trustees and take adequate risk-based measures to verify their identity;

b. identify the trust's ultimate beneficial owner and take adequate risk-based measures to verify the ultimate beneficial owner's identity;

c. establish the objective and intended nature of the business relationship;

d. conduct continuous monitoring consistent with Art.3(2)(d) above;

e. establish that the client is authorised to act as a trustee.

Finally, Art.3(4) contains the CDD requirements to be applied by institutions when the customer acts as a partner of a partnership, including measures to identify the ultimate beneficial owner of the partnership and verify his identity.

R5 (Deficiency 1): (1) There is no direct obligation in the *WWFT* or related legislation requiring financial institutions to determine whether the customer is acting on behalf of another person.

This deficiency is addressed. Deficiency 1 relates to the beneficial ownership requirement in c.5.5.1 and the *WWFT* contains requirements to address this deficiency. In the Netherlands the two categories of customers referred to in R5 are subject to CDD obligations: 1) permanent customers with whom a business relationship is established; and 2) occasional customers who conduct either a one-off transaction of at least EUR 15 000 or two or more related transactions with a joint value of at least EUR 15 000. The set of CDD requirements in Art.3 of the *WWFT* applies to both categories of customers. As regards situations where the customer may be acting for a third party, Art.3(2)(b) & (f) then impose obligations which are broadly similar and which require FIs to identify such third parties and take risk-based measures to verify their identity. Art.3(2)(b) provides for identification/verification of the ultimate beneficial owner, and Art.3(2)(f) specifically requires FIs to implement adequate risk-based measures to verify whether the customer is acting on his own behalf or for a third party. These two provisions meet the deficiency noted in the MER. Both the MoF and DNB guidance papers provide detailed explanations and clarification in view of implementation.

R5 (Deficiency 2): For foreign legal persons "not based in the Netherlands," there is no indication that documents used to verify the identity of a legal entity should be from an "independent" source.

This deficiency is addressed through an amendment to the *WWFT*. Art.11(3) of the *WWFT* has been supplemented with the following specific requirements regarding non-Dutch based foreign legal entities: *"The identity of a client that is a foreign legal person and does not have its registered office in the Netherlands is verified on the basis of reliable documents, data or information which are customary in international commerce and have been obtained from an independent source or documents, data and information that have been recognised as valid means of identification by the State from which the client originates."* This amended provision in the *WWFT* is drafted in a general manner but both the

MoF and DNB guidance documents provide extensive supporting material in view of the implementation of this requirement.

The MoF guidance paper clarifies that foreign companies are registered with the Dutch Chamber of Commerce if they have a branch or commercial undertaking and an establishment in the Netherlands and that relevant identification data can be found in the Commercial Register of the Chamber of Commerce.

Both guidance papers clarify what is meant by *"customary in international commerce"*. For examples of documents which can be considered as "*customary in international commerce"*, both the MoF and DNB guidance paper specifically reference the "Basel Committee on Banking Supervision: General Guide to Account Opening and Customer Identification", February 2003. In addition, the MoF guidance also underlines that institutions need to take the risk associated with the country of incorporation, including because of insufficient company registration requirements, into account. It is clarified that this can for instance be done by relying on relevant findings in reports of international organisations, including the MERs approved by the FATF.

R5 (Deficiency 3): The *WWFT* does not obligate financial institutions to verify that a person purporting to act on behalf of a legal entity is so authorised.

This deficiency is addressed.

Art.3(2)(e) of the *WWFT* requires FIs to establish that the natural person who represents the customer is authorised to do so. Based on Art.3(2)(g), the natural person referred to in sub-section (e) needs to be identified and his/her identity verified. These provisions are clarified in the explanatory memorandum to the *WWFT* amendment: *"The institution needs to determine the extent to which a natural person acting as a client's representative is authorised to represent the client. This is applicable, for example, to the situation in which a natural person acts as the director of a legal person. When a natural person acts on behalf of a legal person that has control of another legal person then the institution shall need to determine the chain of representative authority. The institution shall need to request the natural persons furnish information about their identity and verify their identity."* (*House of Representatives of the States-General, 2011–2012 Sessions, 33 238, No. 3)*.

Section 4.1.3 of the DNB guidance specifically describes the situation where a natural person is acting on behalf of a legal person: *"Where a natural person is acting as a representative of a customer, the institution also checks whether this person is authorised to represent the customer, for example, where a natural person acts as the director of a legal person, the chain of representative authority is established. The customer will subject to the CDD measures in s.3 of the WWFT, while the natural person acting as representative will be identified and his identity verified (s.3(2)(g) of the WWFT)."* The general guidance on the *WWFT* issued by the Dutch MoF also provides similar clarification. As mentioned in footnote 9, the term legal person is defined in commercial legislation to which a specific reference is included in the MoF guidance document.

R5 (Deficiency 4): There is no requirement to obtain a "foreign legal person's" address and legal form, or to obtain the name of trustees or directors or provisions regulating the power to bind the legal person or arrangement.

This deficiency is partially addressed. The obligation to verify the legal status of the legal person can be inferred from the provisions that require identifying and verifying the identity of a customer that is a legal person (Art.3) and the record-keeping requirements (Art.33). Art.33(1)(a), (b) and (c) of the *WWFT* have been amended to provide an overview of the data to be kept in relation to (a) natural persons, (b) legal persons incorporated under Dutch law, and (c) foreign legal persons. These record-keeping requirements include for foreign legal persons, amongst other data, the documents on the basis of which the identity was verified, the natural person who acts on behalf of the legal person, the address as well as the country of their registered office. For legal persons incorporated under Dutch law, the record-keeping obligation explicitly requires a copy of the deed of incorporation. There is no corresponding record-keeping requirement for foreign legal persons and there is no obligation either to obtain the name of directors or provisions regulating the power to bind the foreign legal person. The guidance papers issued and recently updated by the DNB and the MoF contain specific instructions on how to conduct CDD and implement the record-keeping requirements for foreign legal persons, including regarding the nature and form of the documents to rely on. However, as indicated above, these documents do not qualify as OEM.

The Dutch authorities explain that to address the part of the deficiency in relation to trustees, Art.3 of the *WWFT* dealing with CDD measures was supplemented with sub-section 3 which sets out in detail the information that needs to be collected for trusts even though the term customer does not cover legal arrangements. To understand the trust's ownership and control structure, FIs are required to identify the trust's settlors, trustees, and beneficial owners and to take adequate risk-based measures to verify their identity. The MoF guidance also contains relevant instructions in this regard.

R5 (Deficiency 5): The definition of the beneficial owner falls short of the FATF standard as it only refers to legal persons and trusts, and not, more broadly, to the natural person(s) who ultimately owns or controls "a customer". The definition does not refer to the person that can exercise ultimate effective control over a legal arrangement.

The deficiency is addressed. Art.1(f) of the *WWFT*, which contains the definition of *"ultimate beneficial owner"*, has been amended to make specific reference to the natural person(s) who can control the customer. As indicated in footnote 9 above, the term customer covers both natural and legal persons but does not cover trusts or other legal arrangements, which cannot be established in the Netherlands. However, in a trust scenario, the customer is the trustee and both the general CDD requirements as well as specific CDD requirements, including beneficial ownership requirements, apply (see also Art.3(3)). In addition, Art.3(4) also explains the concept of actual control when a customer acts as partner of a partnership.

The definition of *"ultimate beneficial owner"* in the *WWFT* now largely mirrors the definition of beneficial owner in the 3rd EU AML Directive, and beneficial owners have to be identified for all customers, both natural and legal persons. In addition, as explained in detail in relation to

deficiency 3 above, the CDD requirements in Art.3(2)(f) of the *WWFT* oblige FIs to verify whether a customer is acting on behalf of another person.

The guidance documents issued by the DNB and the MoF deal with the identification of the *"ultimate beneficial owner"* and provide concrete examples of documents on which FIs can rely for the identification of beneficial owners of legal persons or trusts. In addition, the guidance documents contain examples to support the implementation of the extended scope of the beneficial ownership requirements to "the natural person(s) who ultimately owns or controls a customer" which could also be a natural person.

R5 (Deficiency 6): The requirement to verify the identity of the beneficial owner and to understand the ownership and control structure of the customer are subject to a risk-based approach and are only applicable in high-risk scenarios.

This deficiency is addressed. The amended Art.3(2)(b) of the *WWFT* provides that an FI shall determine the identity of the *"ultimate beneficial owner"* and implement adequate risk-based measures to verify the *"ultimate beneficial owner's"* identity. When the client is a legal person, FIs are required to implement risk-based and adequate measures to understand the client's ownership and control structure. The Explanatory Memorandum to the *WWFT* clarifies that a FI always needs to determine the identity of the *"ultimate beneficial owner"*, and verify this identity.

In relation to the risk-based measures for verification of the identity of the beneficial owner, the DNB guidance paper specifies that *"The institution also takes adequate risk-based measures to verify the identity of the [ultimate beneficial owner][11] based on independent and reliable documents. This does not mean that the institution has a choice as to whether or not to verify the identity of the ultimate beneficial owner depending on the risk involved: his/her identity must always be verified, but the way in which the verification is carried out will be risk-based. This means that more measures are taken with respect to high-risk customers than to low-risk customers."* The guidance paper issued by the MoF also underlines the obligation to always verify the identity of a customer's *"ultimate beneficial owner"* and to understand the customer's ownership and control structure and provides examples which illustrate how risk-based measures can be implemented in this regard.

R5 (Deficiency 7): Rather than identifying circumstances in which simplified CDD can be conducted, Article 6 of the *WWFT* provides a list of customers/scenarios exempt from the CDD requirements stipulated by Article 3(1) (the obligation to undertake customer due diligence, which, as the authorities confirmed, includes the measures detailed in paragraph 2), Article 3 (3) (a)(b)(d) and (4) and Article 4 (1).

This deficiency is not addressed. The Dutch authorities report that "Art.6 of the *WWFT* has been amended to clarify that all transactions must be assessed to determine whether enhanced CDD should be applied, counter-measures may apply, and whether there are indications that the client may be involved in money laundering or financing of terrorism. In those cases, simplified CDD is not

[11] The translation of the *WWFT* states: *"The institution also takes adequate risk-based measures to verify the identity of the customer based on independent and reliable documents. [...]"* The FATF Secretariat confirms that the original Dutch text of the guidance refers to the verification of the identity of the ultimate beneficial owner and not the customer as mentioned in the English translation.

allowed." However, Art.6(1) reads "Without prejudice to the provisions of Art.8 and 9 (these articles deal with enhanced CDD), institutions do not need to comply with the provisions of Art.3(1), (5) and Art.(4)1 for the following customers […]." Art.3 contains the CDD requirements when establishing a business relationship or conducting a transactions while Art.4 deals with the timing of the CDD. Art.6 contains a defined list of customers to which the provision applies, namely: listed companies; Dutch and EU government agencies; publicly listed legal persons; certain other institutions covered by the *WWFT* or equivalent legislation in another EU Member State, and customers temporarily holding funds in accounts in the name of civil-law notaries, lawyers and other independent legal professions with institutions in the Netherlands or in another EU Member State. It does not mention any other types of customers and, as a result, it can be concluded that simplified CDD in the sense of the FATF standards is not permitted in the Netherlands.

In addition, Art.7(1) of the *WWFT* lists a number of products which are exempted from CDD: *"The provisions of Art.3(1), (5) and Art.(4)1 are not applicable to relationships or transactions relating to […]."* These products correspond to the categories of products which the FATF provides as examples to which it may be reasonable to conduct simplified CDD as set out in the Interpretive Note toR5.

While Art.6 and 7 of the *WWFT* are headed *simplified CDD measures*, as indicated above, they provide that CDD requirements do not apply to certain types of customers or products, unless there is a suspicion of ML/TF or an obligation to apply enhanced CDD applies. This approach is based upon Art.11 of the 3rd EU AML Directive. The only requirement for FIs is to obtain sufficient information to make sure that the circumstances are covered. However, the requirement in the FATF standards is that the country can only create exemptions from AML requirements, including with respect to CDD, if the preconditions (which include showing proven low risk) have been met. Those conditions have not been met and thus the legislative scheme of exemptions, which is different from having simplified measures, is not consistent with c.5.9.

The DNB guidance indicates that the Dutch authorities interpret Art.6 and 7 as providing for simplified CDD in respect of a defined set of customers and products. However, the documents not provide any details of what kind of simplified CDD measures could be applied. This being said, the general guidance paper issued by the MoF clarifies that the provisions in Art.6 and 7 are based on the 3rd EU AML Directive and provide for exemptions of CDD but that under the proposed provisions of the 4th EU AML Directive, such exemptions will no longer be possible. Therefore, for now, although the MoF guidance is oriented to the future, the deficiency as set out in the *WWFT* remains.

R5 (Deficiency 8): There are no obligations for financial institutions to ensure that data and information obtained under the CDD process, such as the client risk profile and contact information, are kept up-to-date.

This deficiency is largely addressed. Art.3(8) – FIs are required to implement adequate risk-based measures to ensure that the information collected during the CDD process about the persons mentioned in sub-sections 2, 3, and 4 is kept up-to-date. While the term persons is not defined in the *WWFT*, a reading of the relevant sub-sections appears to suggest that the term "persons" refers to the customer and ultimate beneficial owner in (2), the trustee, settlor, and ultimate beneficial owner in (3) and the partners in (4). The requirement makes a general referral to information collected

during the CDD process and does not specifically refer to, for instance, the risk profile and contact information.

However, the DNB guidance paper clarifies that during the customer acceptance process, the FI should draw up a risk profile and expected transaction pattern for each customer. It is further explained that it is important that for the duration of the customer relationship, the FI periodically checks whether the customer still fits his risk profile and the transaction pattern is in line with expectations. Financial institutions may tailor the frequency and intensity of the reviews to the customer's risk classification. In addition to periodically updating customer data, FIs are also guided to monitor the customer's accounts and transactions, risk profile, contact information and ultimate beneficial owner information. Such monitoring will allow the institution to gain and maintain an insight into the nature and background of its customers and their financial conduct.

The MoF guidance paper provides that "The data obtained by an institution from standard customer due diligence must be kept up-to-date by the institution. This means that the institution periodically checks and, if necessary, updates the data collected under the customer due diligence requirements of Art.3, including the customer's risk profile, contact information and ultimate beneficial owner(s). In doing so, the institution may proceed in a risk-based manner."

R5 (Deficiency 9): No enforceable obligation to consider filing a suspicious transaction report in the case of failure to satisfactorily complete CDD/terminate business relationship.

This deficiency is addressed. The *WWFT* was amended by adding a new sub-section (4) to Art.16 which provides that a disclosure of an unusual transaction must also be submitted in case of a combination of the following circumstances: (1) failure to satisfactorily complete CDD or a termination of a business relationship and (2) indications that the client is involved in money laundering or terrorist financing. The importance of this additional reporting requirement is further underlined in the guidance paper issued by the MoF.

R5 (Deficiency 10): There are no provisions in the *WWFT* obligating financial institutions to apply CDD to existing customers. Transitional provision exists that considers by default the customers identified under the previous AML/CFT regime as identified under the *WWFT*.

This deficiency is marginally addressed. C.5.17 provides that FIs should be required to apply CDD requirements to existing customers on the basis of materiality and risk and conduct due diligence on such existing relationships. The Methodology contains four categories of examples of when it may be an appropriate time to do so.

The revised Art.38(1) of the *WWFT* prescribes when CDD for existing customers, who were identified based on the provisions of previous AML/CFT legislation which was into force from 1 January 1994 until 31 July 2008, needs to be undertaken. The Dutch authorities clarify that for the implementation of the requirement to apply CDD measures to existing customers, it has classified existing customers into risk categories. The period in which the CDD needs to be completed varies

depending on the category in which the existing customer can be placed[12]. The following periods apply to the four different categories:

a. six months for existing customers governed by the provisions of Art.9 of the *WWFT*. Art.9(1) provides that a Ministerial Order may stipulate that institutions designated by the Order are required to implement extraordinary for customers who are domiciled or established or have their registered office in States designated by the Order because of strategic AML/CFT deficiencies or to transactions, business relationships and correspondent bank relationships in relation to those States. It also provides that the Ministerial order may make a distinction by category of institution. The Dutch authorities report that this provision currently focusses on clients from or transactions with Iran and DPRK;

b. one year for existing customers governed by the provisions of Art.8(1) or Art.8(4). Art.8(1) provides that enhanced CDD needs to be applied when and to the extent that a business relationship or transaction, by its nature or in connection with the State in which the customer is domiciled, established or has its registered office, gives cause to an increased ML/TF risk. A Ministerial Order may designate categories of business relationships and transactions which, by their nature, give cause to an increased ML/TF risk. Art.8(4) provides the basis for enhanced CDD to be applied to customers or their ultimate beneficial owners that are politically exposed persons (PEPs) who are not domiciled in the Netherlands or who do not have the Dutch nationality;

c. two years for existing customers to whom sub-sections (a) and (b) above do not apply and are legal persons with their registered office outside the Netherlands or who act for a trust;

d. on the first available occasion for other existing customers to whom subsections (a) to (c) above do not apply.

It is difficult to conclude that these new requirements are driven by materiality and risk even though the Netherlands refers to four risk categories in Art.38. Moreover, the Netherlands also clarifies that in determining these risk categories, a balance was sought between an exact definition of the risk associated with each individual client and the feasibility of applying the new CDD measures to potentially larger groups of clients.

However, the detailed provisions of Art.38 raise several concerns. Category (a) appears to deal with clients from or transactions with jurisdictions for which the FATF calls on its members to apply counter-measures. The FATF considers these jurisdictions to be high-risk but the *WWFT* provides a period of six months to complete CDD. The length of the period appears to be inappropriate taking into account the risks associated with these countries. It should be noted that institutions are required to take *extraordinary* measures in relation to this category of customers but it is not explained what is covered by the term extraordinary measures. Finally, the legislation provides that the Order may make a distinction for application by category of institution. Although the Order as meanwhile published does not make such distinction, it remains unclear why the legislation should provide the option that the Order would apply to some but not all institutions for customers from high-risk jurisdictions.

[12] The Royal Decree of 9 December 2013 provides that the date from which the deadlines set in Art.38 apply is 1 January 2014.

The Dutch authorities report that Dutch FIs are already under obligations in EU sanctions regulations, specifically with regard to Iran and DPRK, and additional DNB guidance on when enhanced CDD is required based on the periodic FATF public statements[13]. This guidance includes:

a. obtaining additional data about customers and the ultimate beneficial owners that are residents of the relevant countries, including additional information on the purpose and nature of the business relation, the origin of the funds and the source of the assets of the clients or the ultimate beneficial owners;

b. increased frequency of regular revisions and updates of information about clients and the ultimate beneficial owners that are residents of the relevant countries;

c. closer monitoring and control of the business relation and the transactions by clients that are residents of the relevant countries, as well as obtaining additional information about the background and reasons for planned or conducted transactions.

The authorities further report that the Dutch Banking Association has confirmed that following the above-mentioned EU regulations and DNB guidance, its members have already fulfilled all CDD obligations of the *WWFT* with regard to any clients from Iran and DPRK.

Category (b) deals with customers for who enhanced CDD needs to be applied and provides for a period of one year following the Decree to complete the CDD to existing customers is issued. The enhanced CDD refers to customers in or transactions with countries with strategic AML/CFT deficiencies. As a result, the period of one year can also not be justified for this category of higher risk customers and transactions. To accommodate concerns expressed that it was unclear how this provision would be applied to a customer who on 1 January 2014 was not yet higher risk but would become higher risk (or PEP) at a later stage, both the MoF and DNB guidance papers have recently been updated to specifically include that "With regard to customers that only qualify as higher risk at a later time, CDD measures must be applied within a reasonable period of time.

Category (c) seems to imply that legal persons with a registered office outside the Netherlands are automatically higher risk than customers with a registered office in the Netherlands; however, it is not clear on which basis this determination is made. In addition, the *WWFT* refers to a legal person who acts for a trust and this appears to refer to a legal person who is a trustee; however, no further clarification is provided in this regard. Moreover, natural persons who act as trustees are not mentioned in this category and it is unclear why natural persons acting as trustees should be treated differently than legal persons acting as trustees.

Finally category (d) deals with all other customers which the Dutch authorities consider to be lower risk for applying CDD on existing customers. It is difficult to understand on which basis this determination of this lower risk is made.

Art.38(2) makes an exception for business relationships relating to life insurance. Client due diligence of these clients will need to be conducted at least at the time of the payment of the financial benefit to the client (pursuant to the existing regulations CDD is already mandatory for the beneficiary at the time of the payment of the benefit.) The Dutch authorities explain that this exception was made after consideration of the risks associated with life insurance and the burden

13 http://www.toezicht.dnb.nl/en/3/51-223306.jsp.

imposed by possible interim CDD in view of the large number of persons involved. The provision in Art.38(2) appears to suggest that all life insurance contracts are lower risk. However, it is difficult to understand why customers with life insurance policies are per definition lower risk than customers of other FIs. With the aim to mitigate concerns expressed in this regard, the MoF guidance document has recently been updated to clarify that CDD in relation to life insurance contracts needs to be undertaken in all cases where a financial payment is made to the customer.

The recently (January 2014) updated guidance papers now also contain details which guide implementation of the provisions of Art.38. In addition to providing clarification as what is exactly required by Art. 38, the MoF guidance paper also provides examples of situations that should trigger an update of CDD measures regardless as to whether the customer can be associated with one of the four categories above. These examples include instances where a customer is due for a review based on the review process established by the FI, when the FI becomes aware that it lacks sufficient information about an existing customer, where there is a material change in the way the account is operated, or a transaction of significance takes place. While this action by the Netherlands is definitely welcomed, the DNB and MoF guidance documents do not qualify as OEM.

R5 (Deficiency 11): Effectiveness issues in the implementation of preventive measures, regarding: the identification and verification of the beneficial owner.

This deficiency is marginally addressed. The Dutch authorities report that the various guidance papers on the *WWFT* specifically deal with the preventive measures concerning the identification and verification of the beneficial owner with the aim to ensure effective implementation by financial institutions. The Dutch authorities have recently (January 2014) taken additional steps to further clarify the beneficial ownership requirements. As indicated in relation to deficiency 5 above, the guidance documents updated by the DNB and the MoF in January 2014 now indeed deal with the identification of the *"ultimate beneficial owner"*, and provide concrete examples of documents on which FIs can rely for the identification of beneficial owners of legal persons or trusts. In addition, the guidance now also contains examples to support the implementation of the extended scope of the beneficial ownership requirements to "the natural person(s) who ultimately owns or controls a customer" which could also be a natural person. However, given the very recent character of some essential updates, it is too early to assess the implementation of the revised measures.

RECOMMENDATION 5, OVERALL CONCLUSION

The 2011 MER identified 10 technical deficiencies and one effectiveness issue in relation to R5. The Netherlands made important progress since the adoption of the MER with the aim to address the deficiencies identified: six of the technical deficiencies (1, 2, 3, 5, 6, and 9) are now fully addressed, one deficiency (8) is largely addressed, deficiency 4 is partially addressed, deficiency 10 is marginally addressed and deficiency 7 is not yet addressed. The effectiveness issue is only marginally addressed because of the very recent update (January 2014) of the guidance documents in view of effective implementation of the beneficial ownership provisions. The Netherlands' current level of compliance with R5 is assessed to be essentially equivalent to LC.

SPECIAL RECOMMENDATION II – RATED PC

SRII (Deficiency 1): The "collection" of funds to commit a terrorist act is only criminalized if the perpetrator has acquired or actually possessed the funds.

This deficiency is addressed. Based on the findings of the MER, the Netherlands amended its *Criminal Code* to introduce an autonomous TF offence which is largely in line with the FATF standards. The new Art.421(1) of the *Dutch Criminal Code* provides that *"Guilty of terrorism financing is punished with a prison sentence of no more than eight years or a fifth category fine: A person who: (a) intentionally provides himself or another person with means or information or intentionally acquires objects, has objects at his disposal or provides objects to another person, which serve in full or in part, directly or indirectly, to provide monetary support for the commission of a terrorist offence or an offence for the preparation or facilitation of a terrorist offence; and (b) intentionally provides himself or another person with means or information or intentionally acquires objects, has objects at his disposal or provides objects to another person, which serve in full or in part, directly or indirectly, to provide monetary support for the commission of one of the offences defined in the nine Conventions and Protocols listed in the Annex to the TF Convention (the nine Conventions and Protocols are listed one by one in Art.421)."* This provision came into force on 1 September 2013.

The Explanatory Memorandum clarifies that the aim of Art.421 is to criminalise raising funds or providing funds to another person, as defined in Art.2 of the *TF Convention*. The Memorandum states that this is expressed by explicitly including the terms *"collecting"*, *"acquiring possession"* and *"providing to another person"* in the definition of the criminal offence. However, the term *"collecting"* cannot be found in the official translation of the *Criminal Code amendment* but it is confirmed that the element of *"collecting"* is specifically and separately included as "*verzamelt*" ("collects") in the original (Dutch) version of the *Criminal Code amendment*. As a result, the omission of the word *"collecting"* in the official translation can be considered to be a translation issue only.

SRII (Deficiency 2): Article 46 of the *Penal Code* does not sufficiently criminalise the financing of conduct covered by the offences set forth in the nine Conventions and Protocols listed in the Annex to the *TF Convention*.

This deficiency is addressed. As explained above in relation to deficiency 1, the new Art.421 of the *Criminal Code* explicitly criminalises the financing of conduct covered by the offences set forth in the nine Conventions and Protocols listed in the Annex to the *TF Convention*.

SRII (Deficiency 3): The criminalisation of financing of an individual terrorist is only limited to the case in which the financed person has been designated under the UN, EC, or Dutch Sanctions Regulations.

This deficiency is largely addressed. The Dutch authorities explain that in addition to the criminalisation of the financing of designated persons (under UN, EC, or Dutch Sanctions Regulations), the intentional provision of financial support to a person defined in the FATF Glossary as a terrorist is criminalised through the "conditional intent" included in Art.421 of the *Criminal Code*. The authorities further specify that "conditional intent" implies that the terrorist financier consciously accepts the significant likelihood that the resources provided will be used in full or in

part for the commission of terrorist acts. However, the formulation in Art.421 and the explanation by the Dutch authorities make specific reference to *"the commission of a terrorist offence or an offence for the preparation or facilitation of a terrorist offence"* and falls short of the FATF standard which also requires the financing of an individual terrorist *for any purpose*.

SRII (Deficiency 4): Attempt to finance a specific terrorist act is not criminalised.

This deficiency is addressed. Art.45 of the *Criminal Code* criminalises in general an attempt to commit any crime contained within the *Criminal Code*. By adding an autonomous TF offence to the *Criminal Code* through Art.421, all attempts to finance a specific terrorist act are criminalised.

SRII (Deficiency 5): The absence of an autonomous TF offence has a negative impact on the effective investigation and prosecution of terrorism financing activities.

As indicated above, the recently introduced autonomous TF offence came only into force on 1 September 2013 and in combination with the nature of this report, effectiveness of the new TF offence cannot be assessed.

SPECIAL RECOMMENDATION II, OVERALL CONCLUSION

The 2011 MER identified four technical deficiencies and one effectiveness issue in relation to SRII. Since the adoption of the MER, the Netherlands made substantial progress in relation to the criminalisation of terrorist financing through the introduction of an autonomous TF offence in the Dutch *Criminal Code*. Three of the technical deficiencies are now fully addressed while the deficiency in relation to the financing of the individual terrorist is largely addressed. The effectiveness of the implementation cannot yet be assessed. Based on the analysis above, it can be concluded that the Netherlands' current level of compliance with SRII is essentially equivalent to LC.

V. REVIEW OF THE MEASURES TAKEN IN RELATION TO THE KEY RECOMMENDATIONS

RECOMMENDATION 26 –RATED PC

R26 (Deficiencies 1 and 4): (1) The FIU-NL has been a project organisation for almost five years, and the Netherlands have undertaken steps towards the final merger between MOT and BLOM only after the onsite visit. The legal framework for the FIU-NL is not yet fully complete. (4) Governance issues affecting the operational independence of the FIU.

This deficiency is addressed. The Netherlands reported various legal and administrative measures to create the legal framework of the FIU-NL. Although a very complex structure, it appears to provide the necessary guarantees to ensure the FIU-NL's operational independence (c.26.6) and compliance with some other criteria of R26 (c.26.1, c.26.2, c.26.5, and c.26.8).

Art.12 of the amended *WWFT*, which came into force on 1 January 2013, provides for the general legal framework for the establishment of the FIU while Art.13 gives an overview of the responsibilities of the FIU-NL, including the FIU's core functions, guidance to institutions and periodic reports. This primary legislation is further supplemented with an Order of the Minister of

Security and Justice issued on 16 May 2013 (no. 382509) establishing the FIU-NL and assigning the core and management functions of the FIU to the Head of the FIU (the "*2013 FIU-NL Establishment Decree*"). As a result of the government's decision that the FIU-NL would continue to be physically located within the National Police Force, the Minister of Security and Justice issued on 24 May 2013 Order no. 382511 mandating the day to day management of the FIU to the Commissioner of the National Police Force ("the *FIU-NL Mandate")*. Finally, the Commissioner of the National Police Force issued on 28 June 2013 a sub-order to delegate the management of the FIU-NL to the Head of the FIU-NL (the "*FIU-NL Sub-mandate")*. The two Orders, the Mandate and the Sub-mandate all entered into force with retroactive effect on 1 January 2013.

First of all, Art.12(3) of the *WWFT* provides that the Minister of Security and Justice is responsible for the management, organisation and administration of the FIU-NL. Art.12(4) of the *WWFT* further stipulates that the Head of the FIU is appointed, suspended and dismissed by Royal Decree on the recommendation of the Minister of Security and Justice in consultation with the Minister of Finance. The *WWFT* (Art.12(5)) also provides that the FIU-NL's budget is determined by the Minister of Security and Justice in consultation with the Minister of Finance. As indicated above, Art.13 provides a detailed overview of the FIU-NL's responsibilities. The *WWFT* thus provides the legal basis for the establishment and primary processes of the FIU.

Secondly, through the *FIU-NL Establishment Decree*, the Minister of Security and Justice delegated the responsibility for the core functions and the overall management, including decisions on budget and responsibility for personnel, of the FIU-NL to the Head of the FIU.

Third, since the Dutch government decided for management purposes (in terms of personnel, IT, housing, and other supportive services) to keep the physical location of the FIU within the National Police Force, the Minister of Security and Justice issued the *FIU-NL Mandate*. This mandate does not deal with the FIU's core functions but focuses on the overall management of the FIU from a purely business perspective. It specifically gives the authority to the Chief of Police to sub-mandate the control over the FIU-NL to the Head of the FIU. The Dutch authorities further explain that by keeping the FIU-NL, although completely independent and autonomous, within the structure of the National Police Force, the close operational relationship which already existed between the FIU and the police services can be maintained.

Finally, the *FIU-NL sub-mandate* provides the safeguard for the full independence of the FIU by delegating all FIU related management decisions, including budget and staff, to the Head of the FIU.

R26 (Deficiency 2): Instances in which access to data does not allow the FIU to properly undertake its functions.

This deficiency is partially addressed. While the FIU already extended its access to additional administrative and police databases, the Dutch authorities reported various actions set out below aimed at further extending the FIU's powers to access information consistent with c.26.3.

As explained in paragraph 470 of the 2011 MER, the FIU has access to financial, administrative and law enforcement information, although there is no specific power laid down in the *WWFT* or in any other regulation for the FIU to request such information (except from reporting institutions – *WWFT* Art.17). While the Netherlands recently amended the *WWFT*, it has not used this opportunity

to provide a specific legal power to the FIU to get access, directly or indirectly, on a timely basis to administrative, law enforcement and other financial information that it requires to properly undertake its functions.

Nevertheless, the Netherlands has taken action to follow up on the relevant recommendations included in the 2011 MER but some of these actions are still work in progress. The FIU already expanded its access to additional administrative data through newly developed databases, such as *TRACK* which contains data in relation to the supervision of legal entities. The authorities also report that the FIU-NL made an inventory of the additional administrative and commercial databases it could use to add value to its operational tasks. Cost implications related to an expansion of the available databases are currently under consideration.

Moreover, the FIU has already access to all police data by using an IT application of the National Police Force. The information in the police related databases cannot yet be automatically matched with data in the FIU's database. To allow for such automatic matches, the Netherlands reports that the FIU-NL should have direct access to raw police data (without having to use the IT application). It considers such direct access essential for enhancing the effectiveness of the FIU. Therefore, the Head of the FIU is currently discussing with the National Police Force how the FIU-NL can get direct access to the raw data in the police related databases. It is recommended that the Dutch authorities ensure that the results of automatic matches between the FIU and police data are only visible to the FIU. The FIU considers it feasible that it gets actual access to raw police data as well as additional administrative and commercial databases during the first half of 2014.

Finally, the Netherlands reports that the FIU-NL has taken various actions to ensure, where possible, not to leave footprints in databases which are consulted by its staff. These actions are taken to address the concerns expressed in paragraph 441 of the MER, namely that the FIU's data are classified to protect their confidentiality (see also deficiency 3 below) but that by conducting searches in external databases, the existence of FIU information could be revealed. It is clarified that FIU analysts now make use of indirect access to some of the FIU's sources of information (such as municipal records, real estate property, internet searches) when further substantiating the analysis of cases (dealing with the same natural or legal person or a set of related transactions) in view of disseminating them to LEAs. It is further clarified that to avoid detection of FIU searches, analysts can use the internet Research Network (iRN) of the National Police Force.

R26 (Deficiency 3): Shortcomings in the secure protection of data.

This deficiency is partially addressed. To address the concerns expressed regarding the secure protection of data and to comply with the requirements of c.26.7, the Netherlands initiated several actions outlined below, including the introduction and gradual implementation of a new IT system. Some of these actions are also still work in progress.

As announced in paragraph 819 of the MER, the FIU started using a new IT system (GoAML)[14] in May 2011. This system, which also offers many new possibilities for data-examination and analysis, is only accessible by FIU personnel.

[14] GoAML is an intelligence analysis system for FIU's developed by the UNODC. This system is currently being used by 16 FIUs worldwide, and other countries are considering implementing it in the near future.

At the end of 2011/beginning of 2012, an IT security audit of the FIU-NL was carried out by FOX-IT (a Dutch IT security company) and this resulted in a confidential report issued on 13 June 2012. The report contains a list of issues with corresponding recommendations to further enhance the FIU's IT security. One of the main issues dealt with in the report was secure protection of data. Based on this confidential report, the FIU undertook an analysis to assess how the issues mentioned in the report can be addressed. In addition, the financial aspects related to the actions needed were also taken into consideration. The Netherlands reports that the Head of the FIU will ensure that the necessary follow-up measures are implemented by the first half of 2014 with the support of the National Police Force.

In addition, the Dutch authorities report that in November 2012, the level of classification of FIU data was raised from State Secret (in Dutch: *Staatsgeheim*) to State Secret – Secret (in Dutch: *Staatsgeheim – Geheim*) in line with the national data classification regime for sensitive data. This (third highest) classification level prescribes a number of security measures which must be strictly followed, such as the physical security of the FIU's premises, screening of authorised personnel, access to data and related authorisations, etc.

The Dutch authorities assure that the involvement of the National Police Force in the secure protection of FIU data is of a practical nature only without impact on the confidentiality of the FIU data. It underlines that the FIU is fully independent and its core functions are performed without any undue external influence, including from the National Police Force. As explained above in relation to deficiencies 1 and 4, the FIU is physically located within the National Police Force. In that context, it is also the responsibility of the National Police Force to ensure that the FIU's premises, database and related IT tools are securely protected.

R26 (Deficiency 5): Effectiveness issues concerning: (1) operational analysis (lack of prioritisation techniques in a context characterized by large amounts of reports); and (2) dissemination of financial information to law enforcement (the role of the "STRs' in triggering ML investigations and prosecutions, as well as in on-going cases, is very minimal; authorities cannot establish how many of the STRs contribute to the opening of ML/TF criminal investigations; access to STR-information is available to law enforcement for investigation of any type of crime, not just ML/TF).

Effectiveness issue (1) regarding operational analysis, in particular prioritisation techniques in a context characterised by large amounts of reports

The MER contained the following recommendation to address the deficiency above: "Streamline financial analysis, by developing automated-based systems for generating red flags and prioritising the analysis of the data in a more structured way."

The Netherlands has taken important steps to follow up on this recommendation. While progress has clearly been made, the first effectiveness issue is only partially addressed because some aspects of these actions are not yet fully implemented.

As indicated in relation to deficiency 3 above, the GoAML system became operational in May 2011. Apart from that, the FIU-NL has also purchased a Reporting and Analytical tool (the R&A tool) called Cognos (an intelligence and analytical tool developed by IBM). The R&A tool complements the

GoAML system and the FIU started testing the tool on 1 November 2013. It allows for a prioritisation (or red flag) system based on risk profiles and ensures that the FIU is capable to undertake in-depth and more strategic analyses to generate new triggers for law enforcement to follow up on. Once the R&A tool becomes fully operational during the first half of 2014, the FIU will also be in a position to produce instant and real-time reports for dissemination to LEA and provide feedback to reporting entities and supervisory authorities.

The Dutch authorities clarify that based on the GoAML system it was already possible to conduct semi-automatic queries based on risk profiles developed by the FIU analysts. To immediately follow up on the concerns regarding the FIU's analytical capability expressed in the MER, this option was used from May 2011 to November 2013 and allowed for the prioritisation of reports that were disseminated to LEA.

In addition, in June 2013, the FIU started working with the KECIDA[15] team of the Dutch National Forensic Institute to develop sophisticated data analysis tools for data-mining purposes and to have the FIU analysts adopt an intelligence-based approach. The Dutch authorities clarify that this project was carried out as an innovation project in the context of the FIU's ambition to "*stay ahead of the game*" and its on-going efforts to further develop and expand its analytical capabilities and techniques. If proven successful, the results of this project, which is co-financed by the National Coordinator for Security and Counterterrorism, will be implemented by the FIU from 2014 onwards.

Effectiveness issue (2) regarding dissemination of financial information to law enforcement (the role of the "STRs' in triggering ML investigations and prosecutions, as well as in on-going cases, is very minimal; authorities cannot establish how many of the STRs contribute to the opening of ML/TF criminal investigations; access to STR-information is available to law enforcement for investigation of any type of crime, not just ML/TF)

The MER contained the following recommendation to address the second effectiveness issue: "Reconsider the whole "dissemination" system, with a view to emphasise a more streamlined provision of information to law enforcement, on a case-by-case basis, given the minimal role played by the current system of dissemination of STRs in generating new criminal investigations/adding value to existing ones."

While the Dutch authorities took various actions with the aim to address this second effectiveness issue, it appears that so far, this deficiency has only been marginally resolved. The authorities provided general background information on the use of STRs to combat crime more generally, but there are no concrete data to clarify the role of STRs in triggering ML investigations and prosecutions or their use in on-going ML cases.

The Dutch authorities however report that with the implementation of the *GoAML* IT system, the FIU also had to change its STR dissemination system. The FIU now uses the application *BlueView*, which is described as one of the most used applications by the Dutch Police Force, for the dissemination of STR data and making these data easily accessible to all law enforcement authorities. The authorities further clarify that STR data are not only used in the context of ML investigations but that these data also add value to various other crime investigations. In addition, in order to get a better

[15] KECIDA stands for Knowledge and Expertise centre for Intelligent Data Analysis.

understanding of the use of STRs, FIU staff are currently conducting a follow-up exercise to determine the end use of STRs by LEA. This exercise should also enable the FIU to identify more clearly how and to what extent FIU data are used for purposes of combating ML.

The FIU-NL has undertaken many outreach initiatives (seminars, road shows, use of internal communication system of LEAs) to ensure that the end users are familiar with the FIU's new dissemination system and make effective use of the STR information disseminated. Moreover, the Public Prosecutor's Office set up a platform to "signal" and "select" money laundering cases (the S&S meetings) based on FIU disseminations. Every six weeks, a number of LEAs meet to discuss potential new ML investigations and the Dutch authorities report that the data disseminated by the FIU play a crucial role in this regard.

The Netherlands also reports that the FIU is now able to obtain digital feedback that enables the FIU-NL to analyse which STRs disseminated have been opened (viewed) by *BlueView*-users. However, as already mentioned in the MER, opening of STRs disseminated only indicates the number of instances in which law enforcement authorities "consult" the STR data, which can be for any type of (on-going) criminal investigation, not necessarily for ML or TF. More broadly, the degree to which information "disseminated" by the FIU effectively contributes to the opening of new ML/TF-related investigations is still not known.

In 2012, the FIU received more generic feedback on how to improve the quality and structure of the STRs disseminated. The authorities also report that the FIU is currently looking into other information systems used by the National Police Force that can also be used for dissemination of STR data. The Dutch authorities are strongly encouraged to ensure that the use of police information systems does not interfere with the FIU's operational independence. Finally, the FIU provided examples of how it works closely with end-users of STR data with the aim of improving the quality of the STR disseminations.

RECOMMENDATION 26, OVERALL CONCLUSION

The 2009 MER identified four technical deficiencies and two effectiveness issues in relation to R26. As far as the technical deficiencies are concerned, two of these deficiencies related to the operational independence and autonomy of the FIU are fully addressed while the two others are only partially addressed because of work in progress. Based on the information provided, it can also be concluded that one of the effectiveness issues is partially addressed while the second one is only marginally addressed. This can be explained by the fact that various steps were taken to address the effectiveness issues but full implementation has not yet been achieved. However, given the clear progress in addressing the deficiencies identified in the MER, in particular the technical deficiencies related to the FIU's autonomy and operational independence, the Netherlands' current level of compliance with R26 is assessed to be essentially equivalent to LC.

RECOMMENDATION 35 – RATED PC

R35 (Deficiency 1): The Netherlands has not ratified and implemented some provisions of the *Palermo and Vienna Conventions*.

This deficiency is largely addressed. Regarding the implementation of the *Vienna Convention*, the MER identified that while the Netherlands may provide a number of different types of mutual legal assistance with respect to drug-related ML offences, assistance in searching or seizing of property or evidence could only be granted in relation to extraditable offences. At that time, drug related ML was not an extraditable offence under Dutch law and the mentioned forms of assistance could thus not be provided in relation to ML offences under the *Vienna Convention*. As explained in detail below in relation to R36 (deficiency 1), the Netherlands has amended its *Extradition Act* and all ML predicate offences are now extraditable offences.

With regard to the implementation of the *Palermo Convention*, in particular Art.7.1(a), the 2011 MER concluded that while preventive measures and a supervisory regime are in place for banks and non-bank FIs, the legal framework setting out the various obligations especially in relation to customer due diligence measures could be strengthened further. As set out above in relation to R5 in section IV, the Netherlands amended its *WWFT* and significantly strengthened CDD obligations.

R35 (Deficiency 2): The Netherlands has ratified but not fully implemented the *TF Convention* as outlined in the various sections of the report.

This deficiency is largely addressed through the addition of an autonomous TF offence in the *Criminal Code* (see analysis in relation to SRII in section IV above).

RECOMMENDATION 35, OVERALL CONCLUSION

The 2011 MER identified two deficiencies in relation to R35. As explained above, these two deficiencies are largely addressed. The Netherlands' compliance with R35 can therefore be considered to be essentially equivalent to LC.

RECOMMENDATION 36 – RATED PC

R36 (Deficiency 1): In relation to a large number of countries, the Dutch authorities may provide assistance in searching and seizing of evidence only in ML cases involving transnational organized crime or corruption but not any other types of predicate offences.

This deficiency is addressed. As explained in detail in the MER (paragraphs 1299 and 1318), mutual legal assistance involving coercive measures such as searches and seizures of evidence could only be taken on the basis of a multilateral or bilateral treaty providing for search and seizure, or in relation to an extraditable offence. Article 51a of the *Extradition Act* previously established ML as an extraditable offence only if it involved situations within the scope of the *Palermo Convention* (ML cases involving transnational organised crime) or the *Merida Convention* (ML cases involving bribery and corruption). Any other forms of ML, including drug and terrorism related ML, were not expressly covered by Art. 51a and were thus not extraditable offences under Dutch law. As a result, mutual legal assistance (MLA) requests from non-Council of Europe countries or countries with which the Netherlands had not entered into a multilateral or bilateral extradition treaty involving

the seizing of evidence and/or the search of premises could only be satisfied in relation to a very limited number of ML predicate offences.

To address this deficiency, the Netherlands made an amendment to Art.51a of the *Extradition Act* through the *Act of 27 October 2011* which partially amended a number of laws in the field of Security and Justice, including the *Extradition Act*. The ML predicate offences covered in Art.420*bis* – Art.420*quater* of the *Criminal Code* (which correspond to the 21 categories of ML predicate offences as identified by the FATF) are now explicitly mentioned as extraditable offences.

R36 (Deficiency 2): Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands' ability to provide MLA.

This deficiency is largely addressed through the addition of an autonomous TF offence in the *Criminal Code* (see analysis in relation to SRII in section IV above). Given that the amendment came only in force on 1 September 2013, it is too early to notice any possible impact on the Netherlands' ability to provide MLA.

The Netherlands provided updated statistics regarding both incoming and outgoing MLA requests related to ML and terrorism (no specifics on TF). From 2010 to 2012, the Netherlands continued to exchange information in relation to ML and terrorism with over 120 countries. The Netherlands reports that the number of incoming and outgoing MLA requests remained stable and is in line with the number included in the MER. The statistics are included in the two tables below.

Total number of incoming and outgoing requests in 2010-2012			
Offence	**Incoming**	**Outgoing**	**Total**
Terrorism	453	159	612
Money Laundering	1 372	1 998	3 370
Total	**1 825**	**2 157**	**3 982**

Number of Incoming and outgoing requests per offence and per year					
	Terrorism		Money Laundering		
Year	**Incoming**	**Outgoing**	**Incoming**	**Outgoing**	Total
2010	147	53	430	541	1 171
2011	150	46	444	740	1 380
2012	156	60	498	717	1 431
Total	**453**	**159**	**1 372**	**1 998**	**3 982**

R36 (Deficiency 3): Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants.

While the Netherlands reported several actions which are aimed at limiting the negative effect of the scope of legal privilege on the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants, this deficiency is only partially addressed.

The *Act of 24 November 2011* amended Art.25 of the *Act on the Profession of Notaries* and lifted the legal privilege regarding third-party accounts held by notaries. The amendment to this Act was made following complaints by police and public prosecution services that legal privilege in relation to third-party accounts held by notaries hindered criminal investigations and procedures.

In the context of the discussion of the above-mentioned (at that time draft) legislation to amend the *Act on the Profession of Notaries*, the Dutch Parliament asked advice from the Secretary of State for Security and Justice. This advice was provided in a letter sent to Parliament in April 2011 which dealt in detail with the scope of the legal privilege of notaries and lawyers under Dutch law and in a broader international context (the case law of the European Court of Human Rights referred to in the MER). It also assessed possible options for restricting legal privilege; however, only the amendment cited above was enacted.

In addition, a legislative proposal aimed at, amongst other things, reducing the timeframe for court decisions on the scope of legal privilege in cases of seizure of documents from lawyers and notaries has been presented to Parliament in May 2013. The aim of this legislative proposal is providing certainty on the question whether materials can be seized or information gathered from notaries and lawyers within a much shorter time period to ensure that investigations are not hindered by pending proceedings on this question. This draft legislation therefore proposes to introduce specific timeframes to be respected by courts of first instance and appeal when deciding on the applicability of the legal privilege of notaries and lawyers where this is invoked by these professionals.

RECOMMENDATION 36, OVERALL CONCLUSION

The 2011 MER identified three deficiencies in relation to R36. As explained above, one of these deficiencies is fully addressed while the second one is largely addressed and the third one only partially addressed. The Netherlands' compliance with R36 is now considered to have reached a level essentially equivalent to LC.

SPECIAL RECOMMENDATION I – RATED PC

SRI (Deficiency 1): The Netherlands has ratified but not fully implemented the *TF Convention* as outlined in the various sections of this report.

This deficiency is largely addressed. As outlined in the analysis in relation to SRII in section IV above, the Netherlands has introduced an autonomous TF offence in its *Criminal Code* and the current level of compliance with SRII is assessed to be essentially equivalent to LC. In addition, the Netherlands amended its *WWFT* and strengthened its CDD obligations and made important progress in relation to R5 (see analysis in relation to R5 in section IV above).

SRI (Deficiency 2): Minor shortcomings remain in respect of the implementation of UNSCR 1267 and 1373.

Special Recommendation III was rated LC in the MER but four relatively minor deficiencies were mentioned as factors underlying the rating. The Netherlands has taken action towards addressing the four deficiencies. Two of these deficiencies are addressed while two others are not yet addressed. Consequently, deficiency 2 in relation to SR.I can be considered to be partially addressed.

The first deficiency in relation to SRIII referred to the fact that there was insufficient guidance for persons and entities other than FIs that may be holding targeted funds or assets regarding the freezing obligations stemming from the international standard, including the obligation to check client files and databases against those lists. The main concern expressed in the body of the report was that in particular, no guidance specifically relevant to lawyers, accountants and notaries had been issued. This first SRI sub-deficiency is addressed. The May 2013 update of the MoF guidance paper, which applies to all institutions including designated non-financial businesses or professions (DNFBPs), introduced additional information regarding the freezing obligations under both *UNSCR 1267 and 1373* and explains in detail the actions individual institutions are required to take following designations. In addition, the BFI, which is the supervisor for accountants, lawyers and legal service providers, and notaries, issued sector specific guidance which directly refers to the aforementioned guidance paper issued by the MoF.

The fact that FIs other than banks were not always sufficiently supervised for compliance with the EC and domestic Sanctions Regulations was noted as a second deficiency. While the Netherlands has made progress towards improving the supervisory and monitoring regime to meet the SRIII requirement, this second SRI sub-deficiency identified is not yet addressed. The Netherlands reports that its supervisors are aware of this finding. The DNB already made some initial improvements to its monitoring system for FIs other than banks and started outreach, including on-site visits, towards insurers. These thematic supervisory actions conducted in 2012 and 2013 found more than half of the examined insurance companies to be non-compliant with the EU and domestic Sanctions Regulations. However, further actions are needed in view of addressing this sub-deficiency. Other supervisors, in particular those for DNFBPs, do not appear to have taken similar actions.

The third deficiency identified in relation to SR.III is that the freezing obligations under *EC Regulation 881/2001* amended by *EC Regulation 1286/2009* do not expressly extend to funds and assets that are owned or controlled "indirectly" by a designated individual, entity, or organisation. Since the MER, the Netherlands did not introduce any changes in its legal framework to address this deficiency. As a result, situations in which a person is acting on behalf of or based on instructions from a designated person, entity or organisation and thus allows the latter to indirectly control funds or economic resources are still not covered.

To address the concerns as to whether funds and assets are frozen without delay in all instances (in particular, for UN listings under UNSCR 1267) expressed in the fourth SRI sub-deficiency, the Netherlands reports that on 23 March 2013 the relevant national Sanctions Regulation (*Sanctions Regulation Al-Qaida 2011*) was amended to require that freezing actions should be applied without delay to persons or entities upon listing by the UN under UNSCR 1267. The FATF Secretariat verified the original version of the relevant Sanctions Regulation and confirms that the new measures introduced indeed address this fourth SRI sub-deficiency.

SPECIAL RECOMMENDATION I, OVERALL CONCLUSION

The MER identified two deficiencies in relation to SRI. The most important deficiency in relation to the implementation of the *TF Convention* is largely addressed. The second deficiency, which was a spill-over of the deficiencies underlying the LC rating for SRIII, is partially addressed.

The Netherlands' current level of compliance with SRI can be considered to have reached a level essentially equivalent to LC.

SPECIAL RECOMMENDATION V – RATED PC

SRV (Deficiencies 1 and 3): (1) Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands' ability to seize and confiscate property upon foreign request. (3) In TF cases, the shortcomings identified under Special Recommendation II may limit the Netherlands' ability to seize and confiscate property upon foreign requests.

As indicated above in relation to R36 (deficiency 2), these two deficiencies are largely addressed through the addition of an autonomous TF offence in the *Criminal Code* (see analysis in relation to SRII in section IV above). Given that the amendment came only into force on 1 September 2013, it is too early to notice any possible impact on the Netherlands' ability to provide MLA.

SRV (Deficiency 2): Statistics were not sufficiently detailed to determine that the extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.

This deficiency is not yet addressed. The Netherlands reports that it has been focusing on awareness raising amongst relevant stakeholders with the aim to reach better quality in registration of extradition requests. The Netherlands believes that such enhanced quality in registration of extradition requests will provide more clarity regarding the effectiveness of the system in the near future.

SRV (Deficiency 4): Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants.

As indicated above in relation to R36 (deficiency 3), this deficiency is only partially addressed. The Netherlands reported several actions which are aimed at limiting the negative effect of the scope of legal privilege on the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants. These are set out in detail in the description regarding R36.

SPECIAL RECOMMENDATION V, OVERALL CONCLUSION

The MER identified four deficiencies in relation to SRV. The two most important deficiencies which were a spill-over of SRII are largely addressed. Two other deficiencies are not or only partially addressed. Nevertheless, the Netherlands has made notable progress with regard to SRV and the current level of compliance is now assessed to be essentially equivalent to LC.

ANNEX

OVERVIEW OF MEASURES TAKEN REGARDING THE NON-CORE AND KEY RECOMMENDATIONS RATED PC OR NC IN THE MER REPORT BASED ON A REPORT BY THE NETHERLANDS

The information in this annex was presented for information and was not discussed or approved by the FATF Plenary.

The Dutch authorities reported that the following measures have been taken to address the deficiencies related to the other Recommendations rated PC or NC: R.6, R.9, R.12, R.14, R.15, R.16, R.21, R.22, R.24, R.25, R.33, R.34, R.38, and R.39.

RECOMMENDATION 6 – RATED PC

R6 (Deficiency 1): There is no requirement for institutions to ascertain source of wealth and to identify the beneficial owner when the source of wealth is a PEP.

Art.8 and 9 of the *WWFT* deal with enhanced CDD measures. Art.8(4)(b) of the *WWFT* has been amended to include an obligation to implement adequate risk-based measures to establish the source of the assets of the PEP and the funds used for the business relationship or transaction. This new requirement is further clarified in the Explanatory Memorandum to the *WWFT*. In addition, both the MoF and DNB guidance documents contain relevant material to assist FIs with the implementation of the *WWFT* requirements regarding PEPs.

R6 (Deficiency 2): The PEP-related requirements do not apply to non-Dutch PEPs resident in the Netherlands.

Art.8(4) of the *WWFT* has been amended to include non-Dutch PEPs resident in the Netherlands. This new requirement is further clarified in the Explanatory Memorandum to the *WWFT*. In addition, both the MoF and DNB guidance documents contain relevant material to assist FIs with the implementation of the *WWFT* requirements regarding PEPs.

R6 (Deficiency 3): The obligation for financial institutions to have risk based procedures to determine whether a customer is a PEP, does not extend to the case of the beneficial owner.

The amended Art.8(4) of the *WWFT* extends the obligation to have adequate risk-based procedures to determine whether not only a customer but also a beneficial owner is a PEP. This new requirement is further clarified in the Explanatory Memorandum to the *WWFT*. In addition, both the MoF and DNB guidance documents contain relevant material to assist FIs with the implementation of the *WWFT* requirements regarding PEPs.

R6 (Deficiency 4): There is no requirement to obtain senior management approval to continue a business relationship when a customer/beneficial owner becomes a PEP or is found to be a PEP during the course of an already established business relationship.

Art.8(5) of the *WWFT* introduced a new requirement to obtain senior management approval to continue a business relationship when a customer or a beneficial owner becomes a PEP or is found to be a PEP during the course of an already established business relationship. This new requirement is further clarified in the Explanatory Memorandum to the *WWFT*. In addition, both the MoF and DNB guidance documents contain relevant material to assist FIs with the implementation of the *WWFT* requirements regarding PEPs.

R6 (Deficiency 5): The notion of close associate in the Explanatory Memorandum is limited to those who are "publicly known".

The Netherlands has amended the MoF guidance paper which now explicitly states that close associates can be persons who are not publicly known (see paragraph 2.2). It should be noted that this guidance does not qualify as OEM.

RECOMMENDATION 9 – RATED NC

R9 (Deficiency 1): No direct obligation for financial institutions to: (1) immediately receive necessary customer information and; (2) satisfy themselves that copies of CDD documents and data will be available without delay.

Art.5(1)(c) of the *WWFT* has been amended to include the explicit obligation for FIs to obtain information concerning the CDD process from the third party prior to entering into a business relationship or conducting a transaction. This new requirement is further clarified in the Explanatory Memorandum to the *WWFT* and both the MoF and DNB guidance documents provide clarification to assist FIs with the implementation of this new provision.

R9 (Deficiency 2): No obligation for financial institutions to satisfy themselves that the third party is regulated or supervised. There is a presumption that all EU and EEA countries adequately apply the FATF recommendations.

The Netherlands reports that it follows from the amended Art.5(1)(a) of the *WWFT* that it is illegal to rely on a third party in a country outside the EU, unless that country has been designated by the Minister of Finance as having equivalent regulations to those in the Netherlands and having supervision so as to ensure compliance with those regulations. It further clarifies that in the proposal for the 4th AML/CFT Directive, the concept of third country equivalence has however been removed and that, if the proposed text is adopted, the Netherlands will amend *WWFT* accordingly.

R9 (Deficiency 3): No enforceable requirement that ultimate responsibility for CDD should remain within the FI relying on the third party.

The obligation for the FI to obtain information concerning the CDD process from the third party has been introduced in Art.5(1)(c) of the *WWFT* (see deficiency 1 above). If the FI has not obtained the

required information, then the conditions for introduced business have not been fulfilled and the onus is on the FI to apply the regular CDD process consistent with Art.3.

RECOMMENDATION 12 – RATED PC

R12 (Deficiency 1): All DNFBPs (except TCSPs): The shortcomings identified under Recommendation 5 and 10 in section 3 also apply.

Eleven deficiencies identified in relation to R5

See detailed analysis in section IV above.

Deficiency 1 identified in relation to R10: The ambiguity caused by the contradiction between general record retention requirements of seven years and specific requirements relating to financial entities that are of five years or less.

The Netherlands reports that it has amended its guidance papers to clarify the record retention requirements as follows:

- Paragraph 2.7 of the MoF guidance;
- Chapter 7 of the DNB guidance; and
- Paragraph 7.4 of the AFM guidance.

Deficiency 2 identified in relation to R10: The record keeping provisions do not explicitly require that records of transactions should be sufficient to permit reconstruction of transactions sufficient for a prosecution.

The Netherlands reports that Art.33 and 34 of the *WWFT* were amended to include an obligation for FIs to maintain records for five years so that these records are accessible. Records regarding transactions reported as STRs (Art.34) will have to be kept in a manner that allows reconstruction of the transaction.

Deficiency 3 identified in relation to R10: The authorities have no power to extend the retention period if necessary in particular cases.

The Netherlands refers to the fact that no provision in this regard is required by the *3r AML/CFT Directive* and that it has therefore not implemented the corresponding recommendation included in the MER.

R12 (Deficiency 2): All DNFBPs: The shortcomings identified under Recommendations 6, 8, 9 and 11 in section 3 also apply. Effectiveness issues equally apply.

Five deficiencies identified in relation to R6

See progress reported by the Netherlands above.

Two deficiencies identified in relation to R8

The Netherlands did not report any actions to address the two deficiencies identified.

Three deficiencies identified in relation to R9

See progress reported by the Netherlands above.

Two deficiencies identified in relation to R11

The Netherlands did not report any actions to address the two deficiencies identified.

Deficiencies regarding effectiveness

The Netherlands did not report any actions to address the effectiveness issues.

R12 (Deficiency 3): Real estate agents: CDD required only on one party to the transaction is covered, not both the buyer and the seller.

The Netherlands reports that the *WWFT* has been amended per 1 January 2014 to ensure that CDD by real estate agents covers both the buyer and the seller.

R12 (Deficiency 4): Lawyers and Notaries: Exemption of CDD requirements in relation to the first meeting with the client.

The Netherlands reports that, as a matter of principle, the first meeting between a lawyer or notary and a client is exempt from CDD in line with Art.9(5) of the *3rd AML/CFT Directive*. On that basis, the Netherlands decided not to implement the corresponding recommendation in the MER.

R12 (Deficiency 5): TCSPs: (1) No requirements for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. (2) No requirements in relation to the identification of the customer other than the beneficial owner, and enhanced due diligence. (3) No indication to when the retention period should start for records of customer information (if different from the beneficial owner) and business correspondence.

With regard to sub-deficiency 1, the Netherlands clarified that providing a registered office or business address is now included in Art.1 of the *WWFT* as a (stand-alone) service and, as a result, relevant service providers are subject to the *WWFT*, including CDD requirements. In relation to sub-deficiency 2, the Netherlands reported that the Implementing *Regulation on Sound Operational Management of Trust Offices* will be amended by mid-2014 and TCSPs will be required to conduct all CDD requirements, including enhanced CDD. In addition, corresponding record-keeping requirements will apply. The Netherlands did not report any actions to address the third sub-deficiency identified.

RECOMMENDATION 14 – RATED PC

R14 (Deficiency 1): Protection from criminal liability for STR reporting applies in the absence of good faith.

The Netherlands amended Art.19 of the *WWFT* (Art.19(1)) to include the element of good faith in the provision concerning protection from criminal liability. This new requirement is further clarified

in the Explanatory Memorandum to the *WWFT* and both the MoF and DNB guidance documents provide clarification to assist FIs with the implementation of the amended provision.

R14 (Deficiency 2): Protection from civil liability for STR reporting is subject to inappropriate conditions.

Art.20(1) of the *WWFT* now provides protection from civil liability on the condition of reasonable assumption that an STR was made to comply with the *WWFT*. This new requirement is further clarified in the Explanatory Memorandum to the *WWFT* and both the MoF and DNB guidance documents provide clarification to assist FIs with the implementation of the new provision.

R14 (Deficiencies 3 and 4): (3) Tipping-off prohibition does not apply to directors, officers, and employees. (4) Tipping-off prohibition does not apply to information in the process of being reported.

Article 23(1) of the *WWFT* has been amended to extend the tipping-off prohibition to apply to all persons working for an FI, including directors, officers and employees, and to also cover the internal review of transactions to determine whether an STR should be filed or not.

RECOMMENDATION 15 – RATED PC

R15 (Deficiencies 1, 2 and 3): (1) The internal control requirements are mostly to be found in the *Wft* (previous preventive AML/CFT measures which were into force from 1 January 1994 until 31 July 2008) rather than the *WWFT*. The coverage of the *Wft* is not the same as that of the *WWFT* and some of the requirements in the *Wft* (including the requirements for internal controls, internal audit and compliance functions) do not apply to certain categories of regulated financial entities. (2) There is no requirement relating to the seniority or access to managers of the head of the compliance function. (3) The detailed requirements in the *Wft* for compliance functions, relating to their access to resources and documents, their reporting requirements and other matters do not apply to banks with no investment functions and there are no comparable requirements in the *Wgt* (previous preventive AML/CFT measures which were into force from 1 January 1994 until 31 July 2008).

The Netherlands points to the fact that these requirements do not have to be set out in law or regulation. While, as mentioned in the MER, there does not appear to be a practical or effectiveness problem in this area, the deficiency identified has been addressed in the MoF and DNB guidance document. Section 3.4 of the MoF guidance paper covers internal control issues in relation to the freezing and sanctions regulation while section 3 of the DNB guidance document, dealing with the application of the risk-based approach, gives an overview of the requirements and expectations in relation to the internal control function, the internal audit and compliance. It should be noted however that these guidance documents do not qualify as OEM.

R15 (Deficiency 4): The requirements for employee training on AML/CFT in the *WWFT* are limited to the obligation that employees be instructed in the provisions of the *WWFT* and trained to recognize unusual transactions. The broad and general provisions in the *Wft* regarding the provision of information to employees and to business units are not

accompanied by any guidance that makes it clear that training should cover internal policies, procedures and controls, new developments and current ML and TF techniques, methods and trends, as well as all aspects of AML/CFT laws and obligations, including, in particular, requirements on CDD and reporting.

Art.35 of the *WWFT* has been amended to include the obligation to train staff on requirements of the *WWFT*, including CDD requirements, insofar as relevant for the execution of their tasks, and to ensure that staff are trained on a regular basis to be able to recognise unusual transactions and conduct CDD. This obligation is further clarified in the Explanatory Memorandum to the *WWFT*.

RECOMMENDATION 16 – RATED PC

R16 (Deficiency 1): All DNFBPs: The shortcomings identified under Recommendation 13, 14, and 21 in section 3 also apply to DNFBPs.

Deficiency 1 identified in relation to R13: The 14 day period to report after a transaction has been established suspicious does not comply with the requirement of prompt reporting and raises an effectiveness issue in relation to the recovery of criminal assets

Art.16 of the *WWFT* has been amended to explicitly state that STRs must be reported promptly. This requirement is further clarified in the Explanatory Memorandum to the *WWFT* and guidance for implementation is included in the MoF guidance document.

Deficiency 2 identified in relation to R13: Reporting by insurance agents, life insurance companies and bureaux de change is particularly low, which raises concerns regarding the effectiveness of the reporting regime.

The Netherlands reports that in 2012, the number of reports received from bureaux de change had increased with 77% in comparison to 2011 - for details, see the FIU-NL's annual report 2012 at:

http://en.fiu-nederland.nl/sites/en.fiu-nederland.nl/files/u3/FIU%20Annual%20report%202012_ENG.pdf.

It is further reported that the DNB has started outreach to insurers in 2010 and approximately five insurers are examined for AML/CFT compliance per year. In 2012, these examinations took place with a focus on monitoring customers, STR reporting and filtering transactions based on lists related to freezing obligations.

Four deficiencies identified in relation to R14

See progress reported by the Netherlands above.

Three deficiencies identified in relation to R21

See progress reported by the Netherlands below.

R16 (Deficiency 2): All DNFBPs (except TCSPs): (1) No requirement of internal policies, procedures and controls (except lawyers). (2) No requirement to establish an appropriate ongoing employee training. (3) No obligation for an independent audit function to test compliance with the procedures, policies, and controls.

See information reported by the Netherlands in relation to the three deficiencies identified regarding R15 above.

R16 (Deficiency 3): Real estate agents: Reporting requirement only in relation to one party to the transaction, not both the buyer and the seller.

See information reported by the Netherlands regarding R12 (deficiency 3) above.

R16 (Deficiency 4): Lawyers: Inadequate awareness of potential ML vulnerabilities contributing to underreporting.

The Netherlands reports that the Public prosecutor, in cooperation with other relevant agencies such as FIOD, FIU, BFT, and BTW, has started a project that focuses on non-reporting of unusual transactions. It is highlighted that the awareness of lawyers in relation to AML/CFT preventive measures and reporting is increasing. Moreover, a regional supervisory body for lawyers has set up a *WWFT* information centre to assist lawyers with the implementation of the *WWFT* provisions. The Netherlands reports that these steps taken with the aim to improve compliance by lawyers led to an increase in the transactions reported by this category of DNFBPs to the FIU-NL.

R16 (Deficiency 5): TCSPs: (1) No reporting requirements for providing a registered office; business address for a company, a partnership or any other legal person or arrangements, when this service is provided on a standalone basis. (2) Inadequate awareness of potential ML vulnerabilities contributing to underreporting.

As indicated above in relation to R12 (deficiency 5(1)), the Netherlands clarified that providing a registered office or business address is now included in Art.1 of the *WWFT* as a (stand-alone) service and implies that relevant service providers are subject to the *WWFT*, including CDD requirements. The Netherlands did not provide any update regarding the second sub-deficiency.

RECOMMENDATION 21 – RATED PC

R21 (Deficiencies 1 and 3): (1) No specific enforceable obligation for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. (3) The existing counter-measures are limited in scope.

Art.8 of the *WWFT*, which deals with enhanced CDD for all institutions, has been amended to include a reference to the country in which the client resides or is incorporated. The Netherlands reports that a new Art.9 has been added to the *WWFT* to allow for the application of counter-measures with regard to countries with strategic AML/CFT shortcomings by means of a regulation of the Minister of Finance and the Minister of Security and Justice. The new measures are further clarified in the Explanatory Memorandum to the *WWFT*.

R21 (Deficiency 2): No requirement for financial institutions to examine as far as possible the background and purpose of unusual transactions.

The new Art.2(a) in the *WWFT* requires that all FIs subject to the *WWFT* need to give particular attention to transaction patterns which are unusual by their nature and could involve an increased ML/TF risk. The new requirement is also clarified in the Explanatory Memorandum to the *WWFT*.

RECOMMENDATION 22 – RATED PC

R22 (Deficiency 1): There are no provisions requiring the institutions subject to the *WWFT* to apply Dutch standards to branches and subsidiaries in member states of the EU (or EEA).

The Netherlands reports that the provisions of the *WWFT* are in line with the *3rd AML/CFT Directive*. On that basis, the Netherlands decided not to implement the corresponding recommendation in the MER.

R22 (Deficiency 2): The requirement to apply Dutch standards applies only to CDD and not to all appropriate AML/CFT measures.

The Netherlands reports that pending the negotiations on the new EU AML/CFT Directive, the current provision of Art.2(1) of the *WWFT* is maintained in line with Art.31(1) of the *3rd AML/CFT Directive*.

R22 (Deficiency 3): There is no requirement that institutions subject to the Act should pay particular attention to the principle that foreign branches and subsidiaries apply Dutch standards in countries which do not or which insufficiently apply FATF Recommendations.

The Netherlands is of the view that it would be easier to include a requirement to address this deficiency in guidance papers issued by supervisors rather than in legislation. Therefore, an amendment of the *WWFT* in this respect is not foreseen. While the guidance papers indicate that higher (Dutch) standards should be applied, it should be noted that these documents do not qualify as OEM.

R22 (Deficiency 4): The *WWFT* does not require an institution subject to the Act to apply higher host country standards if they exist.

The Netherlands clarifies that it does not deem it necessary to amend the *WWFT* in this regard. Art.2 of the *WWFT* stipulates that institutions must ensure that their branches and subsidiaries in non EU member states must conduct CDD in a manner equivalent to relevant provisions in the *WWFT*. The Dutch authorities further clarify that this should be understood as at least equivalent to. As far as the application of higher host country standards is concerned, the authorities are of the view that this obligation already exists under the laws of the relevant country.

RECOMMENDATION 24 – RATED PC

R24 (Deficiency 1): Secrecy issues prevent the exercise of supervision of lawyers by the designated supervisor.

The Netherlands reports that a Bill, from the State Secretary for Security and Justice, dealing with the supervision of legal professionals is currently under consideration. Parliamentary discussions are expected to start early 2014. It is proposed that an independent Supervisory Board of three persons, which will include one lawyer, will have ultimate responsibility for the supervision of lawyers, including for AML/CFT purposes. The primary supervisory tasks will however be assigned to the local Deans who will act based on binding instructions to be issued by the Supervisory Board. In the performance of their supervisory duties, the Deans will be given the power to override a lawyer's confidentiality duty.

R24 (Deficiency 2): Effectiveness of the measures in place regarding internet casinos illegally operating from the Netherlands could not be fully established.

The Netherlands reports that the Dutch government intends to expand the offer of games of chance, including via the internet. The *Games of Chance Act* (*Wet op de Kansspelen*, *WoK*) does not yet allow internet gambling and offering games of chance on the internet is therefore currently illegal in the Netherlands. The Netherlands clarifies that a legislative proposal regarding a licensing regime for a broad offer of games of chance via the internet was introduced in Parliament. The proposed amendments to the abovementioned Act will not only allow persons to legally gamble on-line but it also provides the competent authorities a legal framework to exercise more control over the providers of internet gambling. It is expected that the proposed new system will not come into force prior to January 2015.

R24 (Deficiency 3): Effectiveness issues in relation to the monitoring of precious metals dealers, lawyers and accountants.

The Netherlands reports that BTW (the Dutch supervisor for dealers in products with high value) shifted the emphasis of its supervision in 2011 to dealers in precious metals and stones because of a recent high demand of silver and gold. The enhanced focus on the monitoring of the precious metals sector resulted in 2012 in a sharp increase of the number of examinations of relevant actors, namely 180 in comparison with 80 in 2011 and 30-35 per year until 2010.

With regard to the effectiveness issue in relation to the monitoring of lawyers, the Dutch authorities make reference to the actions described in relation to deficiency 1 above and indicate that the proposed new Supervisory Board will contribute to addressing this effectiveness issue. Finally, the Netherlands did not provide any data in relation to monitoring of accountants.

RECOMMENDATION 25 – RATED PC

R25 (Deficiencies 1 and 2): (1) Guidance issued to financial institutions is at too high a level of generality to ensure that implementation of AML/CFT defences is adequate and there is a need for more detailed guidance on the nature of AML/CFT risks in the Netherlands, the

importance of establishing a profile and monitoring, and the training and screening of staff. (2) Guidance is, in some respects, out of date, incomplete, and inaccurate.

As indicated in section III.B above, new guidance papers on the *WWFT* have been issued in 2011 and further updated in 2013 and January 2014. A general guidance paper for all institutions has been issued by the MoF while more audience targeted guidance papers were issued by the competent AML/CFT supervisors: DNB, AFM, BFT and BTW. These guidance papers do however not specifically focus on the nature of the AML/CFT risks in the Netherlands.

R25 (Deficiency 3): Feedback to reporting institutions from the FIU is not regarded as sufficient by those institutions.

The Netherlands reports various actions to address this deficiency. As mentioned in relation to R.26 above, providing feedback to reporting entities about trends and relevant phenomena has become a legal obligation and an official task of the FIU-NL through the amended Art.13(c) of the *WWFT*. The Netherlands reports that after discussing the feedback needs of reporting entities with their respective supervisory authorities and professional bodies, it became clear that instead of procedural feedback regarding individual cases, reporting entities preferred more general feedback regarding relevant trends, developments, typologies and phenomena. A separate information leaflet on the changes in the *WWFT* was produced and published on the FIU-NL's website both in Dutch and English: www.fiu-nederland.nl/content/informatiebladen-0. Moreover, an information leaflet regarding so-called Art.17 requests (requests for additional information based on Art.17 of the *WWFT*) was also issued.

By posting examples of cases and best practices on the FIU's website: http://fiu-nederland.nl/casuistiek, the FIU-NL provides specific feedback on how information from reporting entities is being used and in what it results. In addition, during regular direct contacts and so-called "Relation Days", sector specific information is shared with professional bodies and reporting entities. This is done by discussing specific cases, concrete results achieved based on information reported, and relevant trends and phenomena.

In 2013, the FIU-NL also introduced so-called newsflashes which it distributes to a select group of reporting entities through their respective compliance departments. These newsflashes are a more proactive way of informing reporting entities and supervisory authorities of (new) trends and phenomena. They can also be used to draw the attention of reporting entities to certain characteristics of suspicious transactions so they can be more vigilant and use it for future reporting

R25 (Deficiency 4): Specific feedback is not regarded as sufficient by reporting institutions.

The Netherlands reports various actions taken with the aim to address this deficiency. As set out above, to inform and provide feedback to reporting entities on a regular basis, the FIU-NL presents examples of cases and best practices on its website: http://fiu-nederland.nl/casuistiek. Given the diversity of reporting entities, the FIU-NL aims to publish a wide variety of cases. The cases also range from on-going investigations to cases which have been brought to court. All cases presented on the website are labelled, so that the information can be filtered per type of reporting entity. New cases published on the FIU's website appear on top of the "news page" and a twitter message is sent out to inform reporting entities, law enforcement counterparts and other partner agencies.

The Netherlands informs that these case examples have been positively received by reporting entities, professional bodies and supervisory authorities, which frequently make use of the information included in the case examples.

The FIU-NL also has four designated "Relation Managers", responsible for developing and maintaining contacts with their respective reporting institutions, professional bodies and respective supervisors, including during "Relations Days" and providing them with feedback on reports submitted as well as information on new trends and patterns.

As indicated above in relation to the previous deficiency, two general information leaflets for reporting entities in relation to the provisions of the *WWFT* have been produced and published. In addition, and more focused on this specific deficiency identified in the MER, sector specific leaflets have been issued: for instance, an information leaflet on so-called ABC-transactions for notaries; an information leaflet specifically targeting real estate agents; one for trust offices; and another one for "other" traders and dealers. These information leaflets have been distributed both physically (in hard copy) and digitally amongst reporting institutions, with the assistance of the relevant professional bodies and supervisors. The information leaflets are also published on the FIU's website: http://fiu-nederland.nl/content/informatiebladen-0.

RECOMMENDATION 33 – RATED PC

R33 (Deficiency 1): Information on the ultimate beneficial owners of Dutch legal persons is not accessible and/or up-to-date in all cases.

The Netherlands reports various actions taken with the aim to address the deficiency identified. Firstly, the Dutch government recently decided to establish a central shareholders register (*Centraal Aandeelhoudersregister* – Kamerstukken II, 2012/2013, 32608, n° 4) and this register will be operational starting from mid-2015. This register will make it easier to identify the shareholders of private and public limited companies which are not quoted on the stock exchange and to determine the nature of the shares kept by individual shareholders. Amongst other details, the following information will be included in the register: information with regard to the identity of the shareholder; the nature of the share, the unique identification number of the legal person and the related source-documents (e.g. articles of association) on the basis of which registration took place. The Dutch authorities clarify that the central shareholders register will not contain beneficial owner information in all cases but will make it easier to trace the beneficial owners. The central shareholders register will not be public but can be consulted by supervisors and investigative authorities.

On 9 June 2010 the Senate approved the *Bill amending, among other things, Book 2 of the Dutch Civil Code and the Companies (Documentation) Act*. One of the amendments provides for the introduction of a new system of permanent supervision of legal entities. The amendments also extend the scope of the supervision: the new system does not only cover BVs; NVs; and SEs but also other legal entities, such as cooperatives; mutual insurance associations; associations having legal personality; foundations and European Cooperative Societies (SCEs) for which the articles of association provide that they have their registered office in the Netherlands. This supervision also applies to the activities in the Netherlands of a foreign legal entity which has a principal or subsidiary place of business in the Netherlands, as well as the Dutch branches of foreign legal entities. The new

legislation came into force on 1 January 2011 and created an automated information system, called "*TRACK*" which provides detailed information on legal persons created in the Netherlands (see also discussion regarding R26 (deficiency 2)) above.

The new supervision system allows applying scrutiny to legal entities through a risk analysis computer program which allows a dedicated agency - the Scrutiny, Integrity and Screening Agency – to compare legal entities' data with various risk profiles. These entity specific data are obtained by the authorities from both closed and public sources in the Netherlands. The main sources are the system of national registers such as the trade register and the municipal personal records database. In addition, the Ministry of Security and Justice obtains data from the tax authorities, the Judicial Information Service, the Central Insolvency Register and the National Police Services Agency.

If the computer system reveals a heightened risk, either immediately upon registration or later on, during the life span of the entity, the dedicated agency will carry out a more in-depth analysis. If the analysis confirms that there is indeed a heightened risk, a risk alert will be sent to a group of recipients, including law enforcement, supervisory as well as fiscal and social authorities: the Public Prosecution Service; the police; the DNB; the AFM; the tax authorities; as well as special agencies such as the Fiscal Intelligence and Investigation Service/Economic Investigation Service (FIOD/ECD) and the Social Security Information and Investigation Service (SIOD). A risk alert may also be issued at the request of any of these authorities. Whether follow-up action is necessary is decided by the receiving authorities themselves.

R33 (Deficiency 2): The measures that have been put in place to ensure that bearer shares issued by Dutch NVs are not abused for ML or FT purposes are not yet fully effective.

To address this deficiency, the MER recommended that the Netherlands should take necessary measures to ensure that mechanisms are in place to identify the owners of bearer shares or eliminate such shares. The Netherlands reports that the dematerialisation process referred to in paragraph 1231 of the MER was completed on 1 January 2013. As of 1 January 2013, all bearer shares of the majority of Dutch legal persons are electronically registered in the "*girodepot*" at Euroclear the Netherlands or in "*verzameldepots*" of Dutch banks. However, physical bearer shares can still exist for a minority of Dutch legal persons which are not quoted on the stock exchange. To deal with these physical bearer shares, the Netherlands reports to have established an inter-departmental working group with participants from the Ministry of Finance and the Ministry of Security and Justice. This working group is currently carrying out an in-depth analysis to determine the specific challenges presented by bearer shares and to find an appropriate response in order to meet the international standards set by the FATF and the Global Forum on the Transparency of Legal Persons and the Exchange of Information for Tax Purposes.

RECOMMENDATION 34 – RATED PC

R34 (Deficiency 1): For trusts administered by licensed Dutch FIs or DNFBPs, the definition of the "beneficial owners" as contained in the *WWFT* does not extend to "the natural person(s) who ultimately owns or controls a legal arrangement.

As indicated above in relation to R5, Art.3(3) of the *WWFT* contains the CDD measures which institutions are required to take when the customer is acting as a trustee, including identifying the

trust's ultimate beneficial owner and taking adequate risk-based measures to verify the ultimate beneficial owner's identity. The institutions are also required to take adequate risk-based measures to understand the trust's ownership and control structure. In addition, the *WWFT* was also amended to include the new Art.3(4) which provides for specific CDD rules regarding partnerships. Sub-section 3(4)(b) introduces a requirement to identify the natural person who ultimately owns or controls the partnership.

R34 (Deficiency 2): Scope of legal privilege hinders the possibility for law enforcement authorities to access beneficial ownership information regarding trusts held by lawyers, accountants and notaries.

See deficiency 3 in relation to R36 above.

R34 (Deficiency 3): For trusts not administered by Dutch FIs or DNFBPs, the annual updating requirement for beneficial ownership information as required under the Law on Income Tax is not sufficient to ensure that timely, accurate and complete beneficial ownership information is available in all cases.

The Dutch authorities did not report any actions to address this deficiency.

RECOMMENDATION 38 – RATED PC

R38 (Deficiency 1): Although the statistics do not imply that there are significant difficulties in practice, the shortcomings identified under Special Recommendation II may limit the Netherlands' ability to provide MLA.

See deficiency 2 in relation to R36 above.

R38 (Deficiency 2): Scope of legal privilege hinders the possibility for law enforcement authorities to access information and documents held by notaries, lawyers and accountants.

See deficiency 3 in relation to R36 above.

R38 (Deficiency 3): It was not established that the Netherlands effectively seizes and confiscates funds based on foreign request.

The Netherlands reports that a particular focus was placed on awareness raising amongst relevant stakeholders with the aim to reach better quality in registration of seizures and confiscations based on foreign requests. The Netherlands believes that such enhanced quality in registration will provide more clarity regarding the effectiveness of the system in the near future.

RECOMMENDATION 39 – RATED PC

R39 (Deficiency 1): In relation to non-Council of Europe members and countries with which the Netherlands has not signed a multilateral or bilateral extradition treaty, ML offences involving transnational organized crime or corruption are extraditable offences under Dutch law.

See deficiency 1 in relation to R35 and deficiency 1 regarding R36 above.

R39 (Deficiency 2): There is no obligation by Dutch authorities to prosecute a suspect domestically in cases where an extradition request is denied purely on the basis of nationality.

The Netherlands reports that in general it does not deny extradition for purposes of prosecution on the basis of nationality (Art.4(2) of the *Extradition Act*). There is no formal obligation under Dutch law to initiate domestic prosecutions in case of a denial of the extradition request. However, in practice foreign authorities will be contacted about the possibilities of a transfer of proceedings.

R39 (Deficiency 3): Statistics were not sufficiently detailed to determine that the extradition proceedings in the Netherlands are dealt with efficiently and in a timely manner.

See deficiency 2 in relation to SRV above.