CARIBBEAN FINANCIAL ACTION TASK FORCE

Suriname: 1st Enhanced Follow-up Report and Analytical Tool – Rev-2

For approval by written process

Suriname: Follow-up Report with TC Re-ratings & Analytical Tool – Rev-2

Discussion Paper by the Secretariat

Issue	Suriname is undergoing its 1st Enhanced Follow-Up Report (FUR) and is being considered for technical compliance re-rating[1] with five Recommendations.
Recommendation	Delegates are asked to: • Confirm the conclusion to upgrade the rating from PC to C for Recommendations 13 and 21. • Confirm the conclusion to upgrade the rating from PC to LC for Recommendations 12 and 22 • Confirm the conclusion to maintain the rating of PC for Recommendation 10.
Action	If no comments are received, including from the assessed country, the FUR at Annex A will be deemed approved and proceed to publication, in accordance with the procedures as set out in paragraphs 19 and 20 of the CFATF ICRG Procedures for the 4th Round of AML/CFT Evaluations. If two or more delegations (not including Suriname (assessed country)) raise concerns, regarding the Expert's analysis of a particular recommendation in the revised FUR, that recommendation and the issues raised will be discussed at the CFATF November-December 2023 Plenary for consideration

I. Background

Suriname is being considered for TC re-rating on recommendations 10, 12, 13, 21, and 22 which were rated as PC in the MER. The Group of Experts comprising, Mr. Abubakar Nyanzi (Financial Expert), Deputy Head in the AML/CFT Division, Cayman Islands Monetary Authority, Cayman Islands and Mr. Anthony McKenzie, Director, AML/CFT Department, Bank of Jamaica, Jamaica, assessed Suriname's request for TC re-ratings (see the Analytical Tool in Annex B) with the support from Mr. Jefferson Clarke of the CFATF Secretariat.

II. Options

Delegations have two options:

a) Confirm the Group of Experts' analysis and conclusion on the re-rating based on the detailed analysis set out in the Analytical Tool at Annex B (which is not for publication) and reflected in the FUR in Annex A (which is for publication); or

b) Come to different conclusions and agree to amend the FUR to support any new analysis and/or ratings.

III. Analysis

[1] Possible technical compliance ratings: C (compliant); LC (largely compliant); PC (partially compliant); NC (non-compliant); and N/A (not applicable).

Based on the information provided by Suriname, it is concluded that R.13 and R.21 should be upgraded from PC to C and R.12 and R.22 should be upgraded from PC to LC. It is also concluded that R.10 should remain at PC.

IV. Recommendations

Confirm the analysis of the Group of Experts reflected in the FUR in Annex A.

V. Next Steps

Comments were received during the pre-plenary process first circulation. The FUR in Annex A has been revised and is now recirculated. Where no comments are received, the FUR will proceed to publication. However, if two or more delegations (not including Suriname (assessed country) raise concerns, regarding the Group of Experts' analysis of a particular recommendation in the revised FUR, that recommendation and the issues raised will be discussed at the CFATF November-December 2023 Plenary for consideration. Where this report is approved through the pre-plenary written process, Suriname will be directed to report back in November 2024 on its progress.

CFATF Secretariat
October 10, 2023

ANNEX A

Suriname First Enhanced Follow-Up Report – December 2023

1. INTRODUCTION

1. The mutual evaluation report (MER) of Suriname was adopted in December 2022 during the 55th Caribbean Financial Action Task Force (CFATF) Plenary held in the Cayman Islands and published on January 24th, 2023. Since it met the thresholds of having eight or more NC/PC ratings for technical compliance and a low or moderate level of effectiveness for seven or more of the 11 effectiveness outcomes, Suriname was placed under the enhanced follow-up process[2].
2. This FUR analyses the progress of Suriname in addressing the technical compliance requirements of the recommendations being re-rated. Technical compliance re-ratings are given where sufficient progress has been demonstrated. There have been no changes to the requirements relating to the FATF Recommendations.
3. This report does not analyse any progress Suriname has made to improve its effectiveness.
4. The assessment of Suriname's request for technical compliance re-ratings and the preparation of this report was undertaken by the Group of Experts consisting of, Mr. Abubakar Nyanzi (Financial Expert), Deputy Head in the AML/CFT Division, Cayman Islands Monetary Authority, Cayman Islands and Mr. Anthony McKenzie, Director, AML/CFT Department Bank of Jamaica, Jamaica, with the support from Mr. Jefferson Clarke of the CFATF Secretariat.
5. Section 4 of this report summarises the progress made to improve technical compliance. Section 5 contains the conclusion and a table illustrating Suriname's current technical compliance ratings.

[2] Regular follow-up is the default monitoring mechanism for all countries. Enhanced follow-up is based on the CFATF's policy that deals with members with significant deficiencies (for technical compliance and/or effectiveness) in their AML/CFT systems and involves a more intensive process of follow-up.

2. FINDINGS OF THE MUTUAL EVALUATION REPORT & FOLLOW-UP

6. Suriname's MER ratings[3] [4] are as follows:

R.	Rating
1	PC (MER 2023)
2	PC (MER 2023)
3	PC (MER 2023)
4	LC (MER 2023)
5	PC (MER 2023)
6	NC (MER 2023)
7	NC (MER 2023)
8	NC (MER 2023)
9	LC (MER 2023)
10	PC (MER 2023)
11	LC (MER 2023)
12	PC (MER 2023)
13	PC (MER 2023)
14	LC (MER 2023)
15	NC (MER 2023)
16	LC (MER 2023)
17	LC (MER 2023)
18	LC (MER 2023)
19	PC (MER 2023)
20	LC (MER 2023)

R.	Rating
21	PC (MER 2023)
22	PC (MER 2023)
23	PC (MER 2023)
24	NC (MER 2023)
25	NC (MER 2023)
26	PC (MER 2023)
27	PC (MER 2023)
28	PC (MER 2023)
29	PC (MER 2023)
30	PC (MER 2023)
31	PC (MER 2023)
32	PC (MER 2023)
33	LC (MER 2023)
34	C (MER 2023)
35	PC (MER 2023)
36	PC (MER 2023)
37	PC (MER 2023)
38	NC (MER 2023)
39	PC (MER 2023)
40	PC (MER 2023)

7. Given these results and the effectiveness ratings in the MER, Suriname was ~~on~~ placed in enhanced follow-up.

[3] There four possible levels of technical compliance are: compliant (C), largely compliant (LC), partially compliant (PC), and non-compliant (NC). Effectiveness ratings for the 11 Immediate Outcomes are: Low, Moderate (Mod), Substantial or High.

[4] This is Suriname's first request for re-ratings, so the current ratings are indicated based on the original MER.

3. OVERVIEW OF PROGRESS TO IMPROVE TECHNICAL COMPLIANCE

8. In keeping with the CFATF Mutual Evaluation Procedures, this FUR considers progress made up until May 26th, 2023. In line with the ME Procedures and FATF Methodology, the Group of Experts' analysis has considered progress to address the deficiencies identified in the MER and the entirety (all criteria) of each Recommendation under review, noting that this is cursory where the legal, institutional or operational framework is unchanged since the MER or previous FUR.

9. This section summarises the progress made by Suriname to improve its technical compliance by addressing the technical compliance deficiencies identified in the MER.

4. PROGRESS TO ADDRESS TECHNICAL COMPLIANCE DEFICIENCIES IDENTIFIED IN THE MER

4.1.1 Recommendation 10 (originally rated PC)

10. In its 4th round MER, Suriname was rated PC with R.10. The technical deficiencies included: (i) no provision that specify the threshold of USD/EUR 15,000 for carrying out occasional transactions by FIs; (ii) In the insurance context, Suriname had no CDD measures for beneficiaries of life insurance policies; (iii) there is no legislation that requires the FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable; (iv) no measures with respect to: (1) identification and verification requirements for legal arrangements (including their beneficial owners); (2) understanding and, as appropriate, obtaining information on, the purpose and intended nature of the business relationship; (3) understanding the nature of a customer's business and its ownership and control structure for legal persons or legal arrangements; and (4) obtaining information on the powers that regulate and bind legal persons or arrangements; in terms of timing of verification, appropriate risk management procedures are not included; (v) with respect to applying a RBA, there were no SDD measures in place; (vi) there were no measures for a situation were performing CDD will tip off the customer

11. ***Criterion 10.1: (Met)*** No deficiency cited in the MER. FIs were and continue to be prohibited from keeping anonymous accounts or accounts in fictitious names. Since the MER, Suriname made amendments to its AML/CFT framework by establishing the Act on Preventing and Combating Money Laundering and Terrorist Financing ("WMTF Act") in November 2022. The WMTF repealed the WID Act which was applicable at the time of the MER. Service providers are required to do everything necessary to obtain information to establish the identity of those for whom services are provided (art.10 paragraph 1 of the WMTF Act). FIs are required to record information on the first names, address and place of residence or place of business of the client and of the person in whose name an account or a deposit is made (art.20 paragraph 1 of the WMTF Act).

12. ***Criterion 10.2(a) (c) (d) & (e) (Met)*** No deficiency cited in the MER. The requirement for FIs to undertake CDD measures is established at art.7 of the WMTF Act. There are no changes to the AML/CFT framework in this regard.

13. ***Criterion 10.2 (b) (Not met)*** As set out in the MER, the SDUIT does not specify the threshold of USD/EUR 15,000 for carrying out occasional transactions as required by the FATF Recommendations. A service provider is required to undertake CDD measures if it carries out an incidental transaction in or from Suriname for the benefit of the client or if two or more transactions have any connection with a joint value, which is determined by *state decree* (art.7 paragraph 3b of the WMTF Act). The WMTF Act does not specify which is the applicable state decree, whilst the thresholds set out in the SDUIT are in relation to

objective indicators for the purpose of reporting transactions to the FIU (MER paragraph 191). Criterion 10.2(b) remains **Not Met.**

14. ***Criterion 10.3 (Met)*** Suriname did not fully meet this criterion at the time of the MER because there was no specification as to whether the customer includes legal arrangements. Since the MER, Suriname amended its AML/CFT framework and now defines the client as the person being a natural person, a legal entity or any other business arrangement that is not a legal person (art.1 paragraph g of the WMTF Act). This amendment in the definition of the client takes into account legal arrangements.

15. ***Criterion 10.4 (Met)*** No deficiency cited in the MER. FIs were and are required to determine whether the natural person representing the client is authorized to do so and to establish and verify the identity of any third party who is a natural person acting on behalf of the client (art.7 2(e), 2(f) and 2(g) of the WMTF Act).

16. ***Criterion 10.5 (Met)*** Suriname did not fully meet this criterion at the time of the MER because, the requirement for FIs to identify the beneficial owner and take reasonable measures to verify their identity did not include the usage of relevant information or data obtained from a reliable source. Changes made through art.7 2b of the WMTF Act now fully addresses this deficiency.

17. ***Criterion 10.6 (Met)*** Suriname did not fully meet this criterion because, at the time of the MER, there are no provisions for FIs to understand the purpose and intended nature of the business relationship. Changes made through art.7 2c of the WMTF Act addresses now fully address this deficiency.

18. ***Criterion 10.7 (a) (Met)*** No deficiency cited in the MER. FIs were and are required to continuously monitor the business relationship and the transactions carried out during the term of this relationship, in order to ensure that they correspond to the knowledge that the service provider has of the customer and his risk profile, including, if necessary, an investigation into the origin of the resources used in the business relationship or transaction (art.2d of the WMTF Act).

19. ***Criterion 10.7 (b) (Met)*** Suriname did not fully meet this criterion because, at the time of the MER there was ~~is~~ no provision to undertake review of existing records when ensuring CDD information is kept up-to-date and relevant. Art.19 2 of the WMTF Act now fully addresses this FATF requirement.

20. ***Criterion 10.8 (Mostly met)*** For customers that are legal persons and arrangements, the requirement for FIs to understand the nature of the customer's business and its ownership and control structure has been addressed (art.7 paragraph 2b of the WMTF Act). However, there is no explicit direct obligation to understand the nature of the customer's business.

21. ***Criterion 10.9 (a) (b)& (c) (Partly met)*** The deficiency with respect to the exclusion of legal arrangements under criterion 10.9 was addressed with the amendment of art.11 paragraph 1 sub sections a, b, c, and d of the WMTF Act to cover a legal entity or any other form of business arrangement that is not a legal entity. However, in absence of the definition of the term "business arrangement", it remains unclear whether trust-like arrangements are included and covered. Also, there are no provisions for requiring the identification and verification through obtaining information on the powers that regulate and bind the legal person or arrangement as required under c.10.9(b).

22. ***Criterion 10.10 (a) (Met)*** The WMTF Act requires the service provider to identify the ultimate beneficial owners of the client and take adequate measures to verify his identity using relevant information or data obtained from a reliable source, such that the service provider is convinced of the identity of the ultimate beneficial owner (art.7 2b).

23. ***Criterion 10.10 (b) (Met)*** The WMTF Act at art.7 2e, f & g provides for: CDD to determine whether the natural person representing the client is authorised to do so; (f) adequate measures to verify whether the client is acting on his behalf or on behalf of a third party; and (g) where applicable, the identification of the natural person referred to under e and any third party referred to under f and the verification of their identity.

24. ***Criterion 10.10 (c) (Met)*** The WMTF Act at art 11 1d requires that if the client is a legal entity or any other form of business arrangement that is not a legal entity, the identity is established using a certified extract from the Trade Register of the Chamber of Commerce and Industry or using a deed drawn up by a notary established in Suriname. In any case, this extract or deed contains the following information. (b) the decision-makers of the legal person or any other form of business arrangement that is not a legal person, as well as the names of the relevant persons with an administrative and management position within the legal person or any other form of business arrangement that is not a legal person.

25. ***Criterion 10.11 (Not met)*** As noted in the MER, Suriname did not meet the requirements of this criterion as there were no measures for FIs to take identification and reasonable measures to verify the identity of beneficial owners through the following information:

    a) For trust, the identity of the settlor, the trustee (s), the protector (if any), the beneficiaries or class boundaries and any other natural person exercising the ultimate effective control over the trust;

    b) For other types of legal arrangements, the identity of persons in equivalent or similar positions for other types of legal arrangements.

26. Suriname enacted the WMTF Act and advanced arts.10 & 11 as providing adequate measures to satisfy this requirement. It is noted that the obligations prescribed do not provide the specificity relating to the identification of beneficial owners.

27. ***Criterion 10.12 (a) (b) & (c) (Met)*** As noted in the MER, the provisions did not include the requirements for this criterion. Suriname enacted the WMTF Act to correct this by requiring CDD information to be established in the event of concluding, surrendering and paying out, as well as providing intermediary services in the conclusion, surrendering and paying out of a life insurance contract, and of other investment-related insurance products, including: the insured amount and the relevant policy number.

28. ***Criterion 10.13 (Not met)*** As noted in the MER, there are no measures for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

29. ***Criterion 10.14 (Met)*** No deficiency cited in the MER. The timing of verification for customers and beneficial owners is established at art.8 2a of the WMTF ACT. There are no changes to the AML/CFT framework in this regard.

30. ***Criterion 10.15 (Met)*** Pursuant to art.8 2a of the WMTF, a service provider is permitted to enter into a business relationship prior to verification. However, verification must occur before any transactions are carried out. Further, according to art. 8 2c of the WMTF, a service provider that is a bank opens an account before the verification of the customer's identity has taken place, if it guarantees that this account cannot be used before the verification has taken place. The above requirements under the WMTF, that prohibit the utilisation of the business relationship prior to verification, negate the need for the adoption of the risk management procedures under C.10.15.

31. ***Criterion 10.16 (Met)*** No deficiency cited in the MER. The requirement to apply CDD measures to existing customers is established at art.7 2d of the WMTF Act. There are no changes to the AML/CFT framework in this regard.

32. ***Criterion 10.17 (Met)*** No deficiency cited in the MER. A service provider is required to perform enhanced CDD where the ML/TF risks are higher (art.14 of the WMTF Act). There are no changes to the AML/CFT framework in this regard.

33. ***Criterion 10.18 (Met)*** FIs are only permitted to apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the financial institution (art.13 of the WMTF Act). The permitted simplified CDD measures do not apply if the client, business relationship or transaction entails a higher risk of money laundering or terrorist financing or if there are indications that the client is involved in money laundering or terrorist financing (art.13 4 of the WMTF).

34. ***Criterion 10.19 (a) (Met)*** No deficiency cited in the MER. There is an obligation to not open the account, commence the business relationship or perform the transaction or terminate the business relationship, where the FI is unable to comply with relevant CDD measures (art.9 of the WMTF Act). There are no changes to the AML/CFT framework in this regard.

35. ***Criterion 10.19 (b) (Not met)*** As noted in the MER, the requirement for making a disclosure to the FIU was limited to when the service provider (FIs) cannot perform CDD after the business relationship has commenced. Art.9 2 of the WMTF Act provides for the immediate termination of the business relationship and filing of an STR after entering the business relationship. However, there exists no obligation for FIs to consider filing an STR in relation to the customer for failing to provide the relevant CDD information.

36. ***Criterion 10.20 (Met)*** No deficiency cited in the MER. Where a service provider forms a reasonable suspicion of a client's involvement in ML or TF, and they believe that performing the CD could tip-off the client, the service provider is permitted to not pursue the CDD process and is obligated to file a report to the FIU (art.8 3 of the WMTF Act). There are no changes to the AML/CFT framework in this regard.

Weighting and conclusion:

37. Since the MER, Suriname has taken steps to rectify some of the identified gaps. Whilst most of the CDD measures are in place in Suriname, deficiencies still exist in current AML/CFT legislative framework. Suriname has no provision that specify the threshold of USD/EUR 15,000 for carrying out occasional transactions by FIs which is considered a minor deficiency. In the insurance context, there is no legislation that requires the FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. These deficiencies are not weighted heavily based on Suriname's risk and context and the size of the insurance sector. With respect to CDD measures, there are no measures regarding: (1) identification and verification requirements for legal arrangements (including their beneficial owners); (2) understanding the nature of the client's business when performing identification and verification procedures for a legal entity or any other form of business which is not a legal entity; (3) obtaining information on the powers that regulate and bind legal persons or arrangements; (4) regarding a legal entity governed by public law and religious organisation, in addition to the same deficiency as local or foreign entities there is no requirement for obtaining proof of existence; (5) there exists no obligation for FIs to consider filing an STR in relation to the customer for failing to provide the relevant CDD. These deficiencies are weighted heavily as some relate to higher risk areas such as identification and verification of beneficial ownership and proof of existence.

38. **Suriname is re-rated Partially Compliant for R.10.**

4.1.2 Recommendation 12 (originally rated PC)

39. ***Criterion 12.1 (Met)*** No deficiency cited in the MER. The requirement to: put risk management systems in place, to determine whether a client a potential client or the

ultimate beneficial owner is a PEP; obtain senior management approval for the establishment (or continuation for existing customers) of those business relationships; take reasonable steps to establish the source of funds and the source wealth; and to exercise stricter supervision on the business relationship on an ongoing basis, is established at art.16 of the WMTF Act. There are no changes to the AML/CFT framework in this regard.

40. ***Criterion 12.2 (a) & (b) (Met)*** The MER noted that Suriname's legislation did not define or make any reference to the domestic PEPs and there was no defined CDD measures for domestic PEPs or persons who have been entrusted with a prominent function by an international organisation. PEP is now appropriately defined in the WMTF Act (art.1 x). Art.16 1 of the WMTF Act appropriately addresses the requirement for taking reasonable measures to determine whether a client or an ultimate beneficial owner is a PEP. Art.16 3 a, b, c and d provides for cases of higher risk business relationships to be managed in accordance with c.12.2 (b).

41. ***Criterion 12.3 (Met)*** FIs are required to apply the relevant PEP requirements of art.16 mutatis mutandis to family members and close relatives of PEPs (art.16 4 of the WMTF Act). The application of this obligation is clarified in the Explanatory Memorandum for art.16 whereby the PEP requirements extend to close associates of the PEP.

42. ***Criterion 12.4 (Mostly met)*** The MER noted that there was no requirement in Suriname's legislation that requires FIs to determine whether the beneficiaries and/or where required, the beneficial owner of a beneficiary of a life insurance policy is a PEP. Art.8 2b of the WMTF Act requires a service provider that is a life insurer to identify the beneficiary of a policy and verify the identity after the business relationship has been established. In such cases the identification and verification of identity will take place on or before the time of payment or on or before the time at which the beneficiary wishes to exercise his rights under the policy. There is no requirement for senior management involvement before paying out in cases where the beneficiaries have been identified as PEP and no obligation to consider making a STR.

Weighting and conclusion:

43. The deficiencies noted in the 4th round MER have been largely addressed with the amendments made within the WMTF Act. There is, however, no requirement for senior management involvement before paying out in cases where the beneficiaries have been identified as PEPs. Due to the limited risks, the issues relating to life insurance are given minimal weighting. The deficiencies outlined in the 4th Round MER have now been largely addressed with minor shortcomings remaining,

44. **Suriname is re-rated as Largely Compliant for R.12.**

4.1.3 Recommendation 13 (originally rated PC)

45. ***Criterion 13.1 (a) (Met)*** A service provider who intends to enter into a correspondent bank or similar relationship shall ensure that it collects sufficient information about the respondent institution to obtain a full picture of the nature of its business activities and to establish the reputation of the respondent institution and the quality of supervision exercised over that institution, including information about any investigations into ML and TF or measures taken as part of supervision (art.17 1a of the WMTF Act).

46. ***Criterion 13.1 (b) (Met)*** A service provider who intends to enter into a correspondent bank or similar relationship shall ensure that it assesses the respondent institution's procedures and measures to prevent money laundering and terrorist financing and ascertains that these are adequate and effective (art.17 1b of the WMTF Act).

47. ***Criterion 13.1 (c) (Met)*** No deficiency cited in the MER. There is an obligation for a service provider to obtain senior management approval before establishing new

corresponding banking relationships (art.17 2 of the WMTF Act). There are no changes to the AML/CFT framework in this regard.

48. ***Criterion 13.1(d) (Met)*** No deficiency cited in the MER. There is an obligation for a service provider to clearly understand the AML/CFT responsibilities of each institution (art.17 1c of the WMTF Act). There are no changes to the AML/CFT framework in this regard.

49. ***Criterion13.2 (a) & (b)(Met)*** No deficiency cited in the MER. There are requirements with respect to "payable-through accounts" (art.17 3 of the WMTF Act). There are no changes to the AML/CFT framework in this regard.

50. ***Criterion 13.3 (Met)*** No deficiency cited in the MER. FIs are prohibited from entering into or continuing a correspondent banking relation with a shell bank and must satisfy themselves that a respondent service provider do not allow their accounts to be used by shell banks (WMTF Act, art.17 4 and art.17 5 respectively). There are no changes to the AML/CFT framework in this regard.

Weighting and conclusion*:*

51. The deficiencies outlined under Criteria 13.1(a) and 13.1(b) of the 4th Round MER have now been addressed with the enactment of the WMTF Act.

52. **Suriname is re-rated as Compliant with R.13.**

4.1.4 Recommendation 21 (originally rated PC)

53. ***Criterion 21.1 (Met)*** There are provisions that protect service providers, their directors, and their employees, from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by statutory provisions when they report suspicions of ML or related designated criminal offences or TF, insider trading and market manipulation, in good faith to the FIU Suriname (art.36 and art. 37 of the recently enacted WMTF Act).

54. ***Criterion 21.2 (Met)*** No deficiency cited in the MER. Tipping-off and confidentiality obligations with regard to data and information provided or received pursuant to the WMTF Act, including in relation to the filing of STRs, are established at art.45 1 of the WMTF Act. There are no changes to the AML/CFT framework in this regard.

Weighting and conclusion:

55. Suriname has taken significant steps through the passage of the WMTF Act, which include provisions aimed at safeguarding service providers, their directors and their employees, from both criminal and civil liability for breach of any restriction on disclosure of information (including those related to TF) imposed by contract or by statutory provisions. Additionally, the WMTF Act designates information shared under the Act as confidential.

56. **Suriname is re-rated as Compliant with R.21.**

4.1.5 Recommendation 22 (originally rated PC)

57. ***Criterion 22.1 (a) to (e) (Partly met)*** In Suriname DNFBPs fall within the meaning of service provider (art.1a of the WMTF Act) and are required to comply with the CDD requirements set out in R.10. The CDD requirements do not outline any de minimis thresholds. The deficiency identified in the 4th Round MER is related to the use of a de minimis threshold of US$5,000 by game of chance providers when implementing CDD measures. This threshold exceeds the recommended limit of USD/EUR 3,000 (see Category H of the SDIUT). However, it is important to note that although the SDIUT remains in effect, this deficiency has been considered addressed because the WMTF, which does not prescribe a de minimis threshold, supersedes the SDUIT.

58. The deficiencies noted in R.10 have a cascading effect on this criterion. R.10 remains partially compliant, which impacts the rating for C22.1. Not all the measures outlined in R.10 would apply to DNFBPS (eg.C.10.12 and C.10.13). For a detailed review of the deficiencies in R.10, please refer to the re-rating assessment for R.10. The applicable identified deficiencies in R.10 were deemed substantial and had an impact on the rating for C.22.1.

59. ***Criterion 22.2 (Met)*** In the MER, Suriname was rated as being largely compliant with the record keeping requirements of R.11. Since the MER, Suriname enacted the WMTF and the record keeping requirements, which are now detailed in arts.19-21 are in accordance with the requirements of R.11. The record keeping requirements apply to all DNFBPs.

60. ***Criterion 22.3 (Met)*** Under the WMTF Act, DNFBPs have the same PEPs requirements as FIs. The deficiencies identified in C12.2, C.12.3 and C.12.4 of the MER have now been addressed. These deficiencies had a cascading effect on the criterion. On this basis, the deficiencies identified in C.22.3 have now been addressed. Please see the re-rating of R.12 (PEPs) for a full analysis.

61. ***Criterion 22.4 (Met)*** Under the recently enacted WMTF Act, DNFBPs are obligated to adhere to new technology requirements outlined in R.15..

    a) **C15.1 (Met):** Service providers are mandated to take adequate measures to identify and assess the risks of ML and TF that may arise from the development and use of new technologies, products and commercial practices, including new service delivery mechanisms. A risk assessment will also be performed prior to the introduction or use of such technologies, products and commercial practices (art.3 3 of the WMTF Act).

b) **C1.15.2 (Met):**

Sub C.15.2 (a) (Met): As noted in c.15.1, art. 3 3 of the WMTF Act requires that a service provider must undertake risk assessment prior to the introduction or use of new technologies, products and commercial practices.

Sub C.15.2 (b) (Met): There is a general requirement for a service provider to take measures to periodically identify and assess its risks of ML and TF, whereby the measures are proportionate to the nature and size of the service provider (art.3 1 of the WMTF Act)

62. ***Criterion 22.5 (Met)*** Art.12 1 of the WMTF Act stipulates that a service provider is permitted to rely on the due diligence conducted by an intermediary or third party on behalf of a customer. The WID Act, which was in force at the time, did not indicate if DNFBPs are allowed to rely on CDD measures conducted by third parties based overseas. Art.1 1a – e of the WMTF Act outlines the criteria that a service provider must fulfil in order to rely on CDD conducted by a third party.

Weighting and conclusion:

63. Suriname has made significant progress in addressing the deficiencies outlined under c.22.2, c.22.3, c.22.4 and c.22.5 of the 4th Round MER. The provisions established in the WMTF Act have resolved the issues related to these criteria. However, there are still remaining deficiencies related to C22.1 concerning CDD measures outlined in R.10, which have a cascading effect on this criterion. R.10 remains partially compliant. These deficiencies should be addressed.

64. **Suriname is re-rated as Largely Compliant with R.22.**

5. CONCLUSION

65. Overall, Suriname has made significant progress in addressing most of the technical deficiencies identified in its MER and has been upgraded to C on R.13 and R.21; upgraded to LC on R.12 and R.22. R.10 is maintained at PC.

66. A summary table setting out the underlying deficiencies for the Recommendations assessed in this report is included at ***Annex A***.

67. Overall, in light of the progress made by Suriname since its MER was adopted, its technical compliance with the FATF Recommendations is as follows as of December 2023:

R.	Rating
1	PC (MER 2023)
2	PC (MER 2023)
3	PC (MER 2023)
4	LC (MER 2023)
5	PC (MER 2023)
6	NC (MER 2023)
7	NC (MER 2023)
8	NC (MER 2023)
9	LC (MER 2023)
10	PC (MER 2023) **PC (FUR 2023)**
11	LC (MER 2023)
12	PC (MER 2023) ↑ **LC (FUR 2023)**
13	PC (MER 2023) ↑ **C (FUR 2023)**
14	LC (MER 2023)
15	NC (MER 2023)
16	LC (MER 2023)
17	LC (MER 2023)
18	LC (MER 2023)
19	PC (MER 2023)
20	LC (MER 2023)

R.	Rating
21	PC (MER 2023) ↑ **C (FUR 2023)**
22	PC (MER 2023) ↑ **LC (FUR 2023)**
23	PC (MER 2023)
24	NC (MER 2023)
25	NC (MER 2023)
26	PC (MER 2023)
27	PC (MER 2023)
28	PC (MER 2023)
29	PC (MER 2023)
30	PC (MER 2023)
31	PC (MER 2023)
32	PC (MER 2023)
33	LC (MER 2023)
34	C (MER 2023)
35	PC (MER 2023)
36	PC (MER 2023)
37	PC (MER 2023)
38	NC (MER 2023)
39	PC (MER 2023)
40	PC (MER 2023)

68. Suriname has 26 Recommendations rated NC/PC. Suriname will remain in enhanced follow-up based on effectiveness ratings. Suriname's next enhanced follow-up report is due November 2024.

5.1 Annex A: Summary of Technical Compliance – Deficiencies underlying the ratings[5]

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating[6]**
R10	PC (MER) PC (FUR 2023)	• Suriname has no provision that specify the threshold of USD/EUR 15,000 for carrying out occasional transactions by FIs. • In the insurance context, there is no legislation that requires the FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. • With respect to CDD measures, there are no measures with respect to: (1) identification and verification requirements for legal arrangements (including their beneficial owners); (2) understanding the nature of the client's business when performing identification and verification procedures for a legal entity or any other form of business which is not a legal entity; (3) obtaining information on the powers that regulate and bind legal persons or arrangements; (4) regarding a legal entity governed by public law and religious organisation, in addition to the same deficiency as local or foreign entities there is no requirement for obtaining proof of existence; (5) there exists no obligation for FIs to consider filing an STR in relation to the customer for failing to provide the relevant CDD. • In terms of timing of verification, whilst there are measures for the timing of verification, they do not include appropriate risk management procedures.
R.12	PC (MER) LC (FUR 2023)	• There is no requirement for senior management involvement before paying out in cases where the beneficiaries have been identified as PEPs • No obligation to consider making a STR
R.13	PC (MER) C (FUR 2023)	• All criteria are met.
R.21	PC (MER) C (FUR 2023)	• All criteria are met.
R.22	PC (MER) LC (FUR 2023)	• The deficiencies identified in R.10 (Customer Due Diligence) have a cascading effect on this criterion. R.10 remains partially compliant, which impacts the rating for C22.1. • Suriname has not provided indications that the country has identified and assessed the risks of ML/TF that may arise in connection with the development of new products and new business practices. •

[5] Ratings and factors underlying the ratings are only include for those recommendations under review in this FUR.

ANALYTICAL TOOL FOR TECHNICAL COMPLIANCE RE-RATINGS REQUESTS (NOT FOR PUBLICATION)

Instructions for Suriname: Use the first four columns of this table to report back on what actions (if any) have been taken to address the technical deficiencies identified in your mutual evaluation report (MER) (focusing on areas rated NC/PC) and implement new requirements where the FATF Standards have changed since your MER was adopted. As is the case with mutual evaluations, it is the responsibility of the assessed country to demonstrate that its AML/CFT system is compliant with the Recommendations. On this basis, the fourth column should explain the actions taken since the MER was adopted including cross-references to specific legislation, enforceable means, or other relevant mechanisms. All relevant legislation should be submitted with the below table.

Instructions for the [Secretariat/group of experts/review group[6]] responsible for analysing the actions taken by the assessed country: Analyse the information in the first four columns of the table, any additional supporting material provided by the assessed country, and the MER's analysis of other criteria (if any) that are not being reported on as no further action has been taken since the MER was adopted. On that basis, determine whether a re-rating is justified or not. Use the last column of this table to record your analysis and conclusions on the extent to which the actions taken by Suriname address the deficiency or meet the new requirements of the FATF Standards. After each Recommendation for which analysis is being undertaken, set out your conclusions concerning the rating (e.g., whether the rating should be upgraded, downgraded[7] or remain the same). The Secretariat/ review group should also consider the progress taken towards any other Recommendations rated NC/PC for which a re-rating is not being sought.

[6]The CFATF Procedures require a group of experts to analyse and review FURs with TC re-ratings.

[7] Downgrades may be possible in cases where the Standard has changed (and the country is found to have a lower level of compliance against the revised recommendation), or it comes to the attention of the expert review group/ Secretariat that the country has lowered its compliance with the FATF standards during the follow-up process.

Annex B. Analytical Tool – Suriname 1stFUR

Rec.#	**MER Rating & updated rating** (*if already assessed in the follow-up process*)	**Criterion #**	**Deficiency cited in MER / New requirements where FATF Standards have changed since MER** (*Use 1 row per deficiency/new requirement*)	**Actions taken** (*To be filled in by the country*)	**Analysis & conclusions** (*To be filled in by the Secretariat/group of experts/review group*)
Recommendations where the country is seeking an upgrade					

R.10	PC	C.10.1	Met	**General: The new Act for prevention and combatting of Money Laundering and the Financing of Terrorism (O.G. 2022 No. 138) was approved by Parliament on November 19th, 2022. This Act came into force on November 21st,2022 and the MOT Act and WID Act has therefore been repealed. The Act for prevention and combatting of Money Laundering and the Financing of Terrorism is referred to as the WMTF (Wet ter voorkoming en bestrijding van Money Laundering en Terrorisme Financiering) in short. See FUR 1 –Doc 1 - WMTF 2022** (Changed Provision) Criteria 10.1 Service providers are required to conduct CDD pursuant to Article 7 paragraph 1 and 2 of the WMTF: 1.The service provider is obliged to conduct customer due diligence to prevent and combat money laundering and terrorism financing. 2. The customer due diligence includes the following measures: a. identifies the client and verify his identity using reliable, independent documents, data or information; b. identifies the ultimate beneficial owner of the client and take adequate measures to verify his identity using relevant information or data obtained from a reliable source, such that the service provider is convinced of the identity of the ultimate beneficial owner. If the client is a legal entity or any other form of business that is not a legal entity, the service provider must take risk-based and adequate measures to understand the ownership and control structure of the client; c. determines the purpose and intended nature of the business relationship; d. to continuously monitor the business relationship and the transactions carried out during the term of this relationship, in order to ensure that they correspond to the knowledge that the service provider has of the customer and his risk profile, including, if necessary, an investigation into the origin of the resources used in the business relationship or transaction; e. to determine whether the natural person representing the client is authorized to do so; f. takes adequate measures to verify whether the client is acting on his own behalf or on behalf of a third party Article 10 paragraph 1 and 2 of the WMTF states the following on prohibiting financial institutions/service providers from keeping anonymous accounts or accounts in obviously fictitious names: 1. A service provider attunes the customer due diligence to the risk sensitivity of the client for money laundering and terrorism financing. Formulates a risk profile of the client and the	**Criterion 10.1 (Met):** **This criterion was considered Met in the 4th round MER as no deficiency was cited.** Pursuant to section 2I. of the 2016 CBvS Directive (Pg.9), which remains in force, FIs are prohibited from opening any anonymous accounts or accounts under fictitious names on behalf of customers. Further, Suriname made amendments to their AML/CFT framework by establishing the Act on Preventing and Combating Money Laundering and Terrorist Financing ("WMTF Act") in November 2022. The WMTF Act repeals the WID Act. Paragraphs 1 and 2 of Article 7 of the WMTF Act requires service providers to: (1) conduct CDD to prevent and combat ML and TF; and (2) (a) identify the client and verify his identity using reliable, independent documents, data, or information. Further, Paragraph 1 of Article 10 of the WMTF Act requires service providers to do everything necessary to obtain information to establish the identity of those for whom services are provided. Also, under article 20 section 1 of the WMTF Act, service providers, FIs are required to record the following information: the surname, first names, address and place of residence or place of business of the client and of the person in whose name an account or a deposit is made, or of the person who is given access to a safe deposit box, or of the person in whose name a payment or transaction is made, as well as their representatives. Therefore, FIs cannot reasonably administer anonymous accounts or accounts in obviously fictitious names. Criterion 10.1 remains **Met**.

				ultimate beneficial owner. **A service provider will do everything necessary to obtain information to establish the identity of those for whom services are provided.** 2. If the client is a natural person, information to determine the identity as referred to in paragraph 1, including: the family name, the first names, the address, the place of residence, the telephone number, the date of birth, the nationality; the nature, number, date and place of issue of the documents on the basis of which the identity has been established are also recorded. The definition of service providers is stated in Article 1 paragraph1 sub a of the WMTF as follows: a financial, non-financial or virtual asset service provider, being a natural person, a legal person or any other form of business entity that is not a legal person, that is providing services professionally or commercially. Pursuant to section 2 I. (CDD) of the 2016 CBvS-AML/CFT Directive, (Page 9), FIs are prohibited from opening any anonymous accounts or accounts under fictitious names on behalf of customers. See FUR 1 -Doc 2 - CBvS Directive 2016 Doc 2	

R.10	PC	C.10.2(b)	The SDUIT does not specify the threshold of USD/EUR 15,000 for carrying out occasional transactions as required by the FATF Recommendations.	The text with regard to criteria 10.2 (a) remains unchanged and is stated in Article 7 paragraph 3 sub a of the WMTF. Criteria 10.2 (b); Although the SDIUT does not specify to undertake CDD measures when carrying out occasional transactions for the threshold of USD/EUR 15,000 as required by the FATF recommendations Article 7 paragraph 3 sub b of the WMTF clearly stipulates 2 instances when CDD measures are required by FIs: 1. when an occasional transaction is carried out in or from Suriname for the benefit of the client; 2. when two or more transactions have any connection with a joint value, which is determined by State Decree. Article 8 paragraph 1 states that service providers should comply with Article 7 paragraph 2, under a, b and c, before the business relationship is entered into or an occasional transaction as referred to in Article 7 paragraph 3, under b and c is carried out. Article 7 paragraph 2 sub a, b and c refer to the CDD requirements. Article 15 paragraph 1 and 2stipulates that when entering into or monitoring a business relationship and the transactions that are performed during this relationship or the performance of occasional transactions, service providers should pay particular attention to a. business relationships and transactions with clients originating from countries or jurisdictions that do not or insufficiently comply with internationally accepted standards in the field of preventing and combating money laundering and terrorist financing; b. all complex and unusual transactions and any unusual features of transactions that have no explicable economic or legal purpose. 2. If a service provider can reasonably suspect from facts and circumstances that a transaction with a client originating from a country or jurisdiction as referred to in paragraph 1 under a or if a transaction as referred to in paragraph 1 under b occurs, it will perform stricter customer due diligence. See SDUIT as being FUR 1- Doc 3- SDUIT 2013 Measures for service providers to perform CDD are stipulated in the WMTF. The SDIUT sets the indicators for reporting on threshold basis or risk basis. Art 7 par 3 sub b requires that service providers perform CDD when carrying out incidental/ occasional transaction in or from Suriname for the benefit of the client or if two or more transactions have any connection with a joint value, which is determined in the SDIUT.	This criterion was considered Met in the 4th round MER as no deficiency was cited. FIs are required to undertake CDD measures when establishing business relationships according to article 7 subsection 3a of the WMTF Act and section 2 I. of the 2016 CBvS Directive (Pg.8) when entering into a business relationship in or from Suriname. Criterion 10.2 (a) remains **Met**. **This deficiency identified in criterion 10.2(b) is not addressed.** This criterion was considered Not Met in the 4th round MER. The deficiency noted in the 4th round MER has not been addressed and criteria is not met. Pursuant to section 2 I. of the 2016 CBvS Directive (Pg.8), CDD measures should be undertaken when executing incidental transactions in accordance with the applicable threshold established under SDUIT or during electronic transfers of funds. Article 7 subsection 3b of the WMTF requires a service provider to perform CDD if it carries out an incidental transaction in or from Suriname for the benefit of the client or if two or more transactions have any connection with a joint value, which is determined by state decree. However, the SDUIT does not specify the threshold of USD/EUR 15,000 for carrying out occasional transactions as required by the FATF recommendations. Further, the WMTF Act does not specify SDUIT as the state degree and the threshold SDUIT Act sets are for purpose of reporting transactions to the FIU (as opposed to CDD purposes).Criterion 10.2(b) remains **Not Met.** **Experts Response:** The Experts maintains their analysis above, that mirrors the findings in the 4th MER on the following basis: *(1)* **Requirements under the R.10.2(b):** Under R.10.2(b), *"FIs should be required to undertake CDD measures when: (b) carrying out occasional transactions above the applicable designated threshold (USD/EUR 15,000) including situations where the transaction is carried out in the single operation or in several operations that appear to be linked".*

				Threshold for the FIs in accordance with the SDUIT: - Category A: US$10.000 - Category B: US$ 25.000 - Category C: US$ 5.000 - Category D: US$ 2.000 In view of what is regulated as mentioned above and taking into account the threshold as laid down in the SDUIT, CDD is already required where the amount is below the threshold of US$/Euro 15.000 as set out in C10.2(b) for the banking sector (Cat A), the exchange offices (Cat C) and the money transfer offices (Cat D). Paragraph 4 of Article 7 is also applicable, whereby it is stated that the provisions of paragraph 3 apply mutatis mutandis if the amount of a transaction is less than the amount set as an indicator by the State Decree, but the transaction, given its nature, can be regarded as unusual and forms part of a set of related transactions.	(2) *The* Experts acknowledges that the thresholds in the SDUIT for credit institutions, securities institutions, investments companies (Category A – US$10,000), Exchange Offices (Category C – US$5,000) and Money Transfer Companies (Category D – US$ 2,000) falls below the threshold of US$15,000 as required by R.10.2(b). However, the threshold for Life Insurance Companies (Category B –US$25,000) is above the threshold of US$ 15,000 as set under R.10. Therefore, while Cat A, C and D thresholds are below the R.10.2(b) threshold, the threshold for Category B is above the threshold of US 10,000. Further, the WMTF Act does not specify SDUIT as the state degree and the threshold SDUIT Act sets thresholds for purpose of reporting transactions to the FIU (as opposed to CDD purposes). Criterion C.10.2(b) remains **not met**.
				(Changed Provision) Criteria 10.2 (c) on carrying out occasional wire transfer transactions in circumstances is now stated in Article 7 paragraph 3 sub c WMTF requiring that a service provider performs customer due diligence if it carries out an incidental transaction in or from Suriname, being a foreign electronic money transfer worth at least $ 1000 or € 1000 (one thousand US dollars or one thousand Euros);	This criterion was considered Met in the 4th round MER as no deficiency was cited. Section 2 I. of 2016 CBvS Directive (Pg.9 to 13) sets out the designated threshold is USD/EUR 1,000 for cross-border wire transfers for the application of requirements of R.16. Article 7 paragraph 3 sub c of the WMTF Act requires that a service provider performs customer due diligence if it carries out an incidental transaction in or from Suriname, being a foreign electronic money transfer worth at least $ 1000 or € 1000 (one thousand US dollars or one thousand Euros). Criterion 10.2 (c) remains **Met**.
				(Unchanged provision) Criteria 10.2 (d) Regarding the suspicion of ML/TF, regardless of any exemptions or threshold is now stated in Article 7 paragraph 1obligating service provider to conduct customer due diligence to prevent and combat money laundering and terrorism financing. Furthermore Article 7 paragraph 3 sub d, e and f also require service providers (FIs) to perform CDD if there are indications that the client is involved in money laundering or terrorist financing and if there is similar suspicion regarding an existing client.	This criterion was considered Met in the 4th round MER as no deficiency was cited. Article 7 subsection 3d,3e and 3f of the WMTF Act and section 2 I requires FIs to perform CDD if there are indications that the client is involved in money laundering or terrorist financing and if there is similar suspicion regarding an existing client. Criterion 10.2 (d) remains **Met**.

				(Unchanged Provision) Criteria 10.2 (e) regarding doubts about the veracity or adequacy of any exemption or threshold is currently stipulated in Article 7 paragraph 3 sub e. According to section 2 I. of the 2016 CBvS-AML/CFT Directive (Page 8) a. when entering into a business relationship in or from Suriname, FIs should apply CDD-procedures, including the identification and verification of the identity of their customers and, if appropriate, of the ultimate beneficiary, as well as the determination of the origin of their capital). b. carrying out occasional transactions: Pursuant to section 2 I. of the 2016 CBvS Directive (Pg.8), CDD measures should be undertaken when executing incidental transactions in accordance with the applicable threshold established under SDUIT or during electronic transfers of funds. c. carrying out occasional wire transfer transactions in circumstances covered by R.16: Section 2 I. of 2016 CBvS-AML/CFT Directive (Pg.9 to 13) sets out the designated threshold is USD/EUR 1,000 for cross-border wire transfers for the application of requirements of R.16. d. Section 2 I. of 2016 CBvS-AML/CFT Directive requires FIs to perform CDD if there are indications that the client is involved in money laundering or terrorist financing and if there is similar suspicion regarding an existing client.	This criterion was considered Met in the 4th round MER as no deficiency was cited. Under Article 7 subsection 3e of the WMTF Act, FIs are required to perform CDD in cases where there is doubt in the reliability of previously obtained information from the client. Criterion 10.2 (e) remains **Met**.

R.10	PC	C.10.3	There is no specification whether the customer identification requirements include legal arrangements.	(Changed Provision) Article 7 paragraph 1 of the WMTF stipulates the obligation for service providers to conduct customer due diligence to prevent and combat money laundering and terrorism financing. Article 1 paragraph 1 sub g of the WMTF defines a client as follows: the person being a natural person, a legal person or any other business arrangement that is not a legal person, with whom a business relationship is entered into, as well as the person who has a transaction carried out, or for whom a service is provided. Aforementioned definition refers to legal persons and legal entity or legal arrangement. The referral to legal entity or legal arrangement is clarified in the Explanatory Notes under Article 1first paragraph. Furthermore, Article 11 paragraph 1 of the WMTF states that if the client is a legal entity or any other form of business that is not a legal entity, the identity is established using a certified extract from the Trade Register of the Chamber of Commerce and Industry or using a deed drawn up by a notary established in Suriname. Therefore, in the new act the requirements regarding legal arrangements are now included. Section 2 I. of 2016 CBvS-AML/CFT Directive (Pg.8) sets out the identification and verification requirements for customers (whether natural persons or legal entities).	**This deficiency is addressed.** This criterion was Mostly Met in the 4th round MER. Article 1 paragraph 1 sub g of the WMTF has been amended to define the client as the person being a natural person, a legal entity or any other business arrangement that is not a legal person, with whom a business relationship is entered into, as well as the person who has a transaction carried out, or for whom a service is provided. This amendment in the definition of the client takes into account natural persons, legal entities and other forms of business arrangements that are not legal persons. In addition, the 2016 CBvS Directive (Pg.8) sets out the identification and verification requirements for clients (whether a natural person or a legal entity). Articles 10 and 11 of the WMTF sets out identification and verification requirements for clients (whether natural persons, legal entities or other forms of business arrangements that are not legal persons). Article 11 paragraph 1 of the WMTF stipulates establishing the identity of legal entity or any other form of business arrangement that is not a legal entity, based on a certified extract from the Commercial Register of the CCI where that legal entity is listed or with the aid of a deed drawn up by a civil-law notary practising in Suriname. The above amended measures within the WMTF now consider other forms of business arrangement that is not a legal entity. Criterion 10.3 is now **Met.**
R.10	PC	C.10.4	Met	(Changed Provision) Service providers are required to verify if the person purporting to act on behalf of the client is authorised to do so and they should also identity and verify the identity of that person. Article 7 paragraph 2 sub e.: to determine whether the natural person representing the client is authorized to do so. Article 7 paragraph 2 sub g: where applicable, to identify the natural person referred to under e and the third party referred to under f and to verify their identity. Article 11 of the WMTF regards the identification of a legal person or business arrangement that is not a legal person. Sub 1d of this article states that information must be obtained on those who represent the legal parson or any other form of business arrangement that is not a legal person with the service provider. This includes the surname, first names, date of birth, address, place of residence and the document used to establish their identity.	This criterion was considered Met in the 4th round MER as no deficiency was cited. Article 7 subsection 2(e), 2(f) and 2(g) of the WMTF requires FIs to determine whether the natural person representing the client is authorized to do so and to establish and verify the identity of any third party who is a natural person acting on behalf of the client. Criterion 10.4 remains **Met**.

R.10	PC	C.10.5	The requirement for FIs to identify the beneficial owner and take reasonable measures to verify their identity does not include the usage of relevant information or data obtained from a reliable source	(Changed Provision) Article 7 paragraph 2 of the WMTF stipulates that customer due diligence includes the following measures. Article 7 paragraph 2 sub b requires identification of the ultimate beneficial owner of the client and take adequate measures to verify his identity using relevant information or data obtained from a reliable source, such that the service provider is convinced of the identity of the ultimate beneficial owner. If the client is a legal entity or any other form of business that is not a legal entity, the service provider must take risk-based and adequate measures to understand the ownership and control structure of the client; Article 11 paragraph 1 states that if the client is a legal entity or any other form of business that is not a legal entity, the identity is established using a certified extract from the Trade Register of the Chamber of Commerce and Industry or using a deed drawn up by a notary established in Suriname. Article 1 paragraph 1 sub t defines the ultimate beneficial owner as the natural person who is the ultimate or actual owner of, or has control over, a client and/or the natural person on behalf of whom a transaction is carried out. The term also includes the person who exercises ultimate effective control over a legal entity, or any other form of business that is not a legal entity/legal arrangement. Section 2 I. of 2016 CBvS-AML/CFT Directive broadly requires the identification and verification of the identity of ultimate beneficiaries.	**This deficiency is addressed.** The deficiency noted in the 4th round MER has been addressed. Article 7 subsection 2b of the WMTF requires the identification and verification of the ultimate beneficial owner of the client and to take reasonable measures to verify his identity using relevant information or data obtained from a reliable source, such that the service provider is convinced of the identity of the ultimate beneficial owner. The above revised provision complies with the criterion. Also, section 2 I. of the 2016 CBvS Directive broadly requires the identification and verification of the identity of the ultimate beneficiaries. Criterion 10.5 is now **Met.**
R.10	PC	C.10.6	There are no provisions for FIs to understand the purpose and intended nature of the business relationship	(Changed Provision) Article 7 paragraph 2 sub c requires service providers (FIs) to carry out CDD including determining the objective and intended nature of the business relationship. Section 2 I. of 2016 CBvS-AML/CFT Directive and section 2 VI (Complex and large-scale transactions and activities) requires to obtain information on the purpose and intended nature of the transaction.	**This deficiency is addressed.** This Criterion was considered Mostly Met in the 4th round MER. The deficiency noted in the 4th round MER has been addressed. Article 7 subsection 2 c of the WMTF requires service providers to carry out CDD including determining the purpose and intended nature of the business relationship. Criterion 10.6 is **Met.**

R.10	PC	C.10.7(b)	There is no provision to undertake review of existing records when ensuring CDD information is kept up-to-date and relevant.	(Changed provision) Criteria 10.7 (a) (rated MET) is reflected in Article 7 paragraph2 sub d (previously article 2 sub 1d of the WID Act) where measures regarding CDD requires service providers to continuously monitor the business relationship and the transactions carried out during the term of this relationship, in order to ensure that they correspond to the knowledge that the service provider has of the customer and his risk profile, including, if necessary, an investigation into the origin of the resources used in the business relationship or transaction; Criteria 10.7 (b) is stipulated in Article 19 paragraph 2 and 3 obligating service providers to undertake review of existing records and ensuring CDD information is kept up to date and relevant. Article 19 paragraph 2 states that service providers are required to ensure that the data and information obtained in the context of a customer due diligence, in particular those relating to customers, ultimate beneficial owners or business relations that entail a higher risk of money laundering and terrorist financing, are updated and relevant by revising the client database. Article 19 paragraph 3 also obliges a client to immediately inform the service provider of any changes to the documents or data used to establish the identity of the client or the identity of the ultimate beneficial owner. a. Pursuant to Section 2 I. of 2016 CBvS-AML/CFT Directive (page 8) FIs should continue to apply CDD-procedures even after the customer has been identified and should closely examine all transactions performed during their business relationship to be sure that the transactions carried out are in line with the information that the institution has about the business, the risk profile and the origin of the customer's funds. b. Section 2 V. (Record Keeping) of 2016 CBvS-AML/CFT Directive stipulate that the identity data and transaction information should be available to the CBvS at request. FIs are required to retain all necessary records on transactions, both domestic and international, for at least 7 years. Such information must be accessible to permit reconstruction of transactions in question so as to provide evidence for the prosecution of criminal activity.	This criterion was considered met within the 4th round MER as no deficiency was cited. Article 7 subsection 2d requires service providers to continuously monitor the business relationship and the transactions carried out during the term of this relationship, in order to ensure that they correspond to the knowledge that the service provider has of the customer and his risk profile, including, if necessary, an investigation into the origin of the resources used in the business relationship or transaction. Also, section 2 I. of the 2016 CBvS Directive (Pg.8) broadly requires FIs to continue to apply CDD-procedures even after the customer has been identified and should closely examine all transactions performed during their business relationship to be sure that the transactions carried out are in line with the information that the institution has about the business, the risk profile, and the origin of the customer's funds. Criterion 10.7(a) remains **Met**. **This deficiency is addressed.** This Criterion was considered Most Met in the 4th round MER. The deficiency cited in the 4th round MER has now been addressed. Article 19 paragraph 2 requires the service provider to ensure that the data and information obtained in the context of a CDD, in particular those relating to customers, ultimate beneficial owners or business relations that entail a higher risk of money laundering and terrorist financing, updated and relevant by revising the client data base. Additionally, pursuant to section 2 I. of the 2016 CBvS Directive (Pg.8), FIs should continue to apply CDD-procedures on a risk-based approach basis even after the customer has been identified. Criterion 10.7(b) is now **Met.**

				Additionally, pursuant to section 2 I. of the 2016 CBvS-AL/CFT Directive (Pg.8), FIs should continue to apply CDD-procedures on a risk-based approach basis even after the customer has been identified.	
R.10	PC	C.10.8	There are no provisions to understand the nature of a customer's business and its ownership and control structure.	(Changed provision) Article 7 paragraph 2 sub b of the WMTF states that if the client is a legal entity or any other form of business arrangement that is not a legal entity, the service provider must take risk-based and adequate measures to understand the ownership and control structure of the client. Therefore, requiring service providers (FI's) to understand the customer's business and its ownership and control structure. Pursuant to Section 2 I. of the 2016 CBvS-AML/CFT Directive requires the identification and verification of ultimate beneficiaries. Article 7 of the WMTF obligates all reporting entities/service providers (financial and non- financial) to undertake measures, when entering into business relationship with a client, as set forth in paragraph 1. Furthermore paragraph 2 sub a, commences with the requirement to identify and verify the identity of the client and ubo. As set out in Art 1 paragraph 1 sub g a client is defined as follows: the person being a natural person, a legal person or any other form of business that is not a legal person, with whom a business relationship is entered into, as well as the person for whom a service is provided. In the case of a service as referred to under c, point 5, is provided, this includes the person who pays the premium, as well as the beneficiary (regarding life insurance). The WMTF does not make a distinction between natural person, legal person or legal arrangement in the definition of "a client". Additionally, Art 7 par 2 sub c and d also requires service providers to determine the purpose and nature of the business relationship and ongoing monitoring of the business relationship as well as transactions carried out during the term of the business relationship in order to ensure that this corresponds with the knowledge that the service provider has of the client and his risk profile, including, if necessary, an investigation into the origin of the resources used in the business relationship or transaction.	**This deficiency is partly addressed.** This Criterion was considered Partially Met in the 4th round MER. The deficiency cited in the 4th round MER has now been partly addressed. Article 7 paragraph 2b of the WMTF requires that if the client is a legal entity or any other form of business which is not a legal entity, the service provider must take risk-based and adequate measures to understand the ownership and control structure of the client. However, this provision does not include an explicit requirement for the service providers to understand the nature of the client's business when performing identification and verification procedures for a legal entity or any other form of business which is not a legal entity. While the CDD obligations prescribed under Article.11 of the WMTF obligates the service provider to establish the identity of the legal entity using a certified extract from the Trade Register of the Chamber of Commerce, the certified extract captures very limited information on the business activity of the customer and there is no direct obligation to understand the nature of the customer's business. Section 2 I. of the 2016 CBvS Directive also requires the identification and verification of ultimate beneficiaries. Criterion 10.8 is now **Mostly Met**. **Experts Response:** The Experts maintains their analysis above on the following basis: (1) **Requirements under the R.10.8:** Under R.10.8, *"For customers that are legal persons or legal arrangements, the FI should be required to understand the nature of the customer's business and its ownership and control structure".* The Experts are of the view there are two requirements within R10.8 i.e..: (1) understanding the nature of the customer's business; and (2) understanding the nature of customer's ownership and control structure. (2) The Experts acknowledges that Article 7 paragraph 2b of the WMTF requires that if the client is a legal entity or any other form of business which is not a legal entity (i.e., for Legal Persons and Legal Arrangements as required under R10.8), the service provider must take risk-based and adequate measures to understand the ownership and control structure of the

				By requiring service providers to comply with the measures set forth in the abovementioned paragraphs service providers should gain a better understanding of the nature of the client's business when performing identification and verification procedures for a legal entity or any other form of business which is not a legal entity. Quoted from the column Analysis and Conclusion of the review group and experts under criteria 10.9: "The deficiency with respect to the exclusion of legal arrangements under criterion 10.9 was addressed with the amendment of Article 11 paragraph 1 sub sections a,b,c, and d of the WMTF to cover a legal entity or any other form of business arrangement that is not a legal entity"	client (Requirement 2). However, this provision does include the expectations under Requirement 1 above (i.e., Understanding the nature of the customer's business). On that basis, this minor deficiency led to this criterion to be rated as **Mostly Met**. For avoidance of doubt, the Experts note that deficiency is not linked to the exclusion of the Legal Arrangements deficiency under Criterion 10.9. (3) **Other points raised by Suriname Authorities:** The Authority acknowledges Suriname's reference to Art.7 para 2 sub c and d of the WMTF Act. However, these provisions relate to separate and distinct requirements under Criterion R.10.6 (Met) and R.10.7(a)(Met).

R.10	PC	C.10.9	There is no specification as to whether the customer includes legal arrangements.	(Changed provision) Criteria 10.9 (a, b and c) are reflected in Article 11 paragraph 1 sub a, b, c and d of the WMTF. This article covers both the legal entity and other forms of business arrangements: 1. If the client is a legal entity or any other form of business arrangement that is not a legal entity, the identity is established using a certified extract from the Trade Register of the Chamber of Commerce and Industry or using a deed drawn up by a notary established in Suriname. In any case, this extract or deed contains the following information: a. the legal form, the statutory name, the trade name, and proof of existence; b. the decision-makers of the legal person or any other form of company that is not a legal person, as well as the names of the relevant persons with an administrative and management position within the legal person or any other form of company that is not a legal person; c. the address, place and country of the registered office and – if different – the main place where the activities are carried out. d. of those who represent the legal person or any other form of company that is not a legal person with the service provider: the surname, first names, date of birth, address, place of residence and the document used to establish their identity. Criteria 10.9 with regard to the right to exist of Legal persons and Legal arrangements.	**This deficiency is partly addressed.** This Criterion was considered Partially Met in the 4th round MER. The deficiencies cited in the 4th round MER have now been partly addressed. The deficiency with respect to the exclusion of legal arrangements under criterion 10.9 was addressed with the amendment of Article 11 paragraph 1 sub sections a,b,c, and d of the WMTF to cover a legal entity or any other form of business arrangement that is not a legal entity. However, in absence of the definition of the term “business arrangement”, it remains unclear whether trust-like arrangements are included and covered. Article 11 sub section 1 of the WMTF requires that if the client is a legal entity or any other form of business arrangement that is not a legal entity, the identity is established using a certified extract from the Trade Register of the Chamber of Commerce and Industry or using a deed drawn up by a notary established in Suriname. In any case, this extract or deed contains the following information: (1) the legal form, the statutory name, the trade name, and proof of existence; (2) the decision-makers of the legal person or any other form of business arrangement that is not a legal person, as well as the names of the relevant persons with an administrative and management position within the legal person or any other form of business arrangement that is not a legal person; (3) the address, place and country of the registered office and – if different – the main place where the activities are carried out; (4) of those who represent the legal person or any other form of business arrangement that is not a legal person with the service provider: the surname, first names, date of birth, address, place of residence and the document used to establish their identity.

				In this context, Article 2 of the Trade Register Act specifies which entities are required to register in the commercial register. For each of the various legal forms, the requirements are regulated separately in the law before they can be registered in the commercial register: Art 5 sole proprietorship Art 6 de VOF Art 7 Partnership and limited partnership Art 8 limited liability company Art 9 cooperative association Art 10 association recognized as a moral body Art 11 return insurance or guarantee company Art 12 matters belonging to a foreigner or legal person established under the legislation of another country It can be concluded from Articles 24 and 25 that registration in the Trade Register is the right of existence of such entity. The sanction provision included in the relevant articles should also be taken into consideration if the registration obligation has not been met, as well as incorrect or incomplete statement at the time of registration in the Trade register. Existence foundations/Law on foundations Article 1 paragraph 1 indicates that the foundation is a legal entity. Art 3 and 4 states requirements for establishing the foundation Art 9 stipulates the registration in the foundation register	Article 11 sub section 2 of the WMTF requires that if the client is a legal person under public law, the identity can also be established by a statement from the administrative body, if it concerns a Surinamese legal person under public law, or a statement from the competent authority, if it concerns a foreign legal person under public law. This statement, which according to its date may not have been issued more than six months in advance, shall in any case include the following information, where applicable: (1) the date of issue; (2) of the legal entity: the name, the legal regulation or the decision from which the legal person under public law derives its legal personality, the address, the place and the country of residence; (3) of those who represent the legal entity at the service provider: surname, first names, date of birth, address, place of residence, position, the document by which their identity has been established, as well as the document on the basis of which the authority to represent of the legal person under public law with regard to the relevant service; (4) of the person issuing the statement on behalf of the administrative body or the competent authority: the surname, first names, date of birth and position. Article 18 of the WMTF requires service providers, when performing enhanced CDD, to perform the following before establishing a business relationship or transaction with a non-profit organisation: (1) ensure that the non-profit organisation has written objectives; (2) establish the true identity of the persons responsible for the activities of the non-profit organisation; and (3) have procedures in place to determine the source of the non-profit organisation's assets and the beneficial owner. The above provisions for identifying and verifying the identity of local or foreign legal entities registered in Suriname and foreign legal entities not also registered in Suriname complies with the requirements of criterion 10.9(a) and10.9 (c). However, there are no provisions for requiring the identification and verification through obtaining information on the powers that regulate and bind the legal person or arrangement as required under Criterion 10.9(b). Regarding a legal entity governed by public law and non-profit organisation, in addition to the same deficiency as local or foreign entities there is no requirement for proof of existence as required under Criterion 10.9(a). Criteria 10.9 remains **Partly Met.** **Experts Response:** The Experts acknowledges reference to the Trade Register Act. However, the Experts notes that there is no direct link between the Trad Register Act and the deficiencies noted with respect to the expected the requirements under the WMTF Act as such

					Criteria 10.9 remains **Partly Met**. Specifically, the Suriname Authorities should kindly refer us to the provisions under the WMTF Act that satisfy the following requirements: 1. **For local or foreign legal entities registered in Suriname and foreign legal entities not also registered in Suriname** - Provisions within the WMTF Act for requiring the identification and verification through obtaining information on the powers that regulate and bind the legal person or arrangement as required under criterion 10.9(b). 2. **For a legal entity governed by public law and non-profit organization** - Provisions within the WMTF Act for requiring the identification and verification through obtaining information on the powers that regulate and bind the legal person or arrangement as required under criterion 10.9(b). Provisions the require for proof of existence as expected under criterion 10.9 (a).
R.10	PC	C.10.9(b)	There are no measures for information on legal arrangements or on the powers that regulate and bind legal persons or arrangements	Please see text above on criteria 10.9	Refer to the text above. All the deficiencies under criteria C.10.9 within the 4th Round MER have not been addressed and thus criterion remains partly met.

R.10	PC	C.10.10 (b) & (c)	There are no measures for the alternatives under sub-criteria 10.10 (b) and (c).	(Changed provision) Criteria 10.10 (a) is reflected in Article 7 paragraph 2 sub b requiring service providers (FI's) to identify the ultimate beneficiary and verify his identity using reliable, independent documents, data or information. Furthermore, FI's are required to identify the ultimate beneficial owner of the client and take adequate measures to verify his identity using relevant information or data obtained from a reliable source, such that the service provider is convinced of the identity of the ultimate beneficial owner. If the client is a legal entity or any other form of business that is not a legal entity, the service provider must take risk-based and adequate measures to understand the ownership and control structure of the client. As defined in Article 1 paragraph 1 sub g a client can be a natural person, a legal person or any other business entity that is not a legal person, with whom a business relationship is entered into, as well as the person who has a transaction carried out, or for whom a service is provided. In case a service, as referred to under c, point 5, is provided, this includes the person who pays the premium, as well as the beneficiary. Criteria 10.10 (b) Article 7 paragraph 2 describes the mandatory requirements for CDD. Article 7 paragraph 2 sub a and b requires the identification and verification of the identity of the client as well as the UBO. Specifically stated under sub b where the client is a legal entity or any other form of business that is not a legal entity a service provider should take necessary measure to understand the ownership and control structure of the client. Additionally sub e, f and g obligate service providers to identify and verify the identity of a third party on whose behalf is being acted upon when conducting a business relationship. As to whom a beneficial owner is, Article 1 paragraph 1 sub t defines the term ultimate beneficial owner: The natural person who is the final or actual owner or who has the authority over a client, and/or the natural person on behalf of whom a transaction is being conducted. The term also includes the person who ultimately performs the factual controls of a legal entity or any other form of business that is not a legal entity. Criteria 10.10(c) Where no natural person is identified service providers are required to determine the identity of the relevant natural person who holds the position of senior managing official in accordance with Article 11 paragraph 1 sub d stating: of those who represent the legal person or any other form of company that is not a legal person with the service provider: the surname, first names, date of birth, address, place of residence and the document used to establish their identity.	**This deficiency is addressed.** This Criterion was considered Mostly Met in the 4th round MER. Article 7 subsection 2b of the WMTF requires the identification and verification of the ultimate beneficial owners of the client and take adequate measures to verify his identity using relevant information or data obtained from a reliable source, such that the service provider is convinced of the identity of the ultimate beneficial owner. Section 2 I. of the 2016 CBvS Directive requires the conduct of CDD measures, including the identification and verification of the identity of the ultimate beneficial owner. The above provision complies with the requirement of sub-criterion 10.10 (a). Article 7 subsection e, f and g of the WMTF, requires the service providers to conduct CDD which includes the following measures: (e) to determine whether the natural person representing the client is authorised to do so; (f) Takes adequate measures to verify whether the client is acting on his behalf or on behalf of a third party; (g) Where applicable, to identify the natural person referred to under e and third party referred to under f and verify their identity. The above provisions comply with the requirement of sub-criterion 10.10 (b) Article 11 sub section 1d of the WMTF requires that if the client is a legal entity or any other form of business arrangement that is not a legal entity, the identity is established using a certified extract from the Trade Register of the Chamber of Commerce and Industry or using a deed drawn up by a notary established in Suriname. In any case, this extract or deed contains the following information. (b) the decision-makers of the legal person or any other form of business arrangement that is not a legal person, as well as the names of the relevant persons with an administrative and management position within the legal person or any other form of business arrangement that is not a legal person; The above provision comply with the requirement of sub-criterion 10.10 (c) on the basis that it includes a requirement to identify and verify any other relevant natural person who the position of senior management official for a legal person or legal arrangement in cases where there is no natural person identified under criterion 10.10(a) and 10.10 (b). Criteria 10.10 is now **Met**.

				a. Pursuant to Section 2 I. of the 2016 CBvS-AML/CFT Directive requires that FIs the conduct of CDD measures, including the identification and verification of the identity of the ultimate beneficial owner.	

R.10	PC	C.10.11	There are no measures for FIs to take identification and reasonable measures to verify the identity of beneficial owners through the following information: (a) For trust, the identity of the settlor, the trustee (s), the protector (if any), the beneficiaries or class boundaries and any other natural person exercising the ultimate effective control over the trust; (b) For other types of legal arrangements, the identity of persons in equivalent or similar positions for other types of legal arrangements.	(Changed Provision) As to sub criteria 10.11 (a and b) reference is made to the Article 7 paragraph 1, which states that service providers are obliged to conduct customer due diligence to prevent and combat money laundering and terrorism financing. Article10 paragraph 1: A service provider attunes the customer due diligence to the risk sensitivity of the client for money laundering and terrorism financing. Formulates a risk profile of the client and the ultimate beneficial owner. A service provider will do everything necessary to obtain information to establish the identity of those for whom services are provided. Article 11 paragraph 1: If the client is a legal entity or any other form of business that is not a legal entity, the identity is established using a certified extract from the Trade Register of the Chamber of Commerce and Industry or using a deed drawn up by a notary established in Suriname. In any case, this extract or deed contains the following information: a. the legal form, the statutory name, the trade name, and proof of existence; b. the decision-makers of the legal person or any other form of company that is not a legal person, as well as the names of the relevant persons with an administrative and management position within the legal person or any other form of company that is not a legal person; c. the address, place and country of the registered office and – if different – the main place where the activities are carried out. d. of those who represent the legal person or any other form of company that is not a legal person with the service provider: the surname, first names, date of birth, address, place of residence and the document used to establish their identity. As part of the whole CDD process service providers are required to adopt the following measures in accordance with Art 7 of the WMTF: Par 2 sub e: to determine whether the natural person representing the client is authorized to do so; Par 2 sub f: take adequate measures to verify whether the client is acting on its own behalf or on behalf of a third party; Par 2 sub g: where applicable, identify the natural person referred to under e and the third party referred to under f and verify their identity. Reference is made to the definitions set by the FATF for the following terms: Settlor: natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.	**The deficiencies are not addressed.** This Criterion was considered Not Met in the 4th round MER. The deficiencies cited in the 4th round MER have not been addressed. With regard to customers that are legal arrangements, there are no measures for FIs to take identification and reasonable measures to verify the identity of beneficial owners through (a) trust, the identity of the settlor, the trustee (s)the protector (if any), the beneficiaries or class boundaries and any other natural person exercising the ultimate effective control over the trust. (b) for other types of legal arrangements, the identity of persons in equivalent or similar positions. The measures cited by Suriname relate to a separate and distinct requirement under criteria 10.9. Criteria 10.11 is remains **Not Met**. **Experts Response:** The Experts maintains its analysis above on the following basis: 1. **Requirements under the R.10.11:** Under R.10.11, *"For customers that are legal arrangements, the financial institution should be required to identify and take reasonable measures to verify the identity of beneficial owners through the following information: (a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership); (b) for other types of legal arrangements, the identity of persons in equivalent or similar positions."* The Experts notes that R.10.11 makes explicit reference to Trusts and other types of legal arrangements and such provisions are not included within the WMTF Act. Further the WMTF Act refers "any other form of business arrangement that is not a legal entity. In the absence of a

				Trustee: the terms trust and trustee should be understood as described in and consistent with art 2 of the Hague convention on the law applicable to trusts and their recognition. Trustees may be professional (e.g. depending on the jurisdiction, a lawyer or trust company) if they are paid to act as a trustee in the course of their business, or non-professional (e.g. a person acting without reward on behalf of family). Subsequently art 2 of the Hague convention reads as follow: For the purpose of this convention, the term 'trust' refers to the legal relationship created – inter-vivos or on death – by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose. A trust has the following characteristics: a) The assets constitute a separate fund and are not a part of the trustee's own estate; b) Title to the trust assets stand in the name of the trustee o in the name of another person on behalf of the trustee; c) The trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.	definition of business arrangement it is unclear whether trustee-like services are included and covered. However, C.10.11 is concerned with the identification of the beneficial owner of the Legal Arrangement. 2. **Other points raised by Suriname Authorities:** The GOE acknowledges Suriname's reference to Art.11 para 1 sub a,b,c and d of the WMTF Act. However, these provisions relate to separate and distinct requirements under Criterion R.10.9. The additional articles reference relating to Article 7 Para 2 sub section e, f, g of the WMTF Act are also separate and distinct requirements under Criterion R.10.4.

R.10	PC	C.10.12	In addition to the CDD measures required for the customer and the beneficial owner, financial institutions should be required to conduct the following CDD measures on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated: (a) for a beneficiary that is identified as specifically named natural or legal persons or legal arrangements – taking the name of the person; (b) for a beneficiary that is designated by characteristics or by class or by other means – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout; (c) for both the above cases – the verification of the identity of the beneficiary should occur at the time of the payout.	Criteria 10.12 (a,b and c). The definition of client (Article 1 paragraph 1 sub g) also extends to the person who pays the premium, as well as the beneficiary when concluding, commuting and paying out, as well as providing mediation in the conclusion, surrendering and paying out of a life insurance contract and other unit-linked insurance products (Article 1 paragraph 1 sub c5). In this regard the definition for beneficiary should also be taken into consideration (Article 1 paragraph 1 sub bb): a natural person, legal entity, or any other form of company which is not a legal entity or category of persons to whom benefits are paid under an insurance policy when/if an insured event covered by the policy occurs. As for the information that needs to be obtained when identifying a client Article 10 and Article 11 apply. Additionally, Article 20 paragraph 1 sub a, b and c of the WMTF states that every service provider is obliged to record the following data: a. the surname, first names, address and place of residence or place of business of the client and of the person in whose name an account or a deposit is made, or of the person who is given access to a safe deposit box, or of the person in whose name a payment or transaction is made, as well as their representatives; b. the nature, number and date of issue of the document used to establish identity, unless Article 20 paragraph 2 applies; c. the nature of the service. Paragraph 2 sub e of Article 20 WMTF states that in addition to the information referred to in paragraph 1 of this article, the following information must also be established with regard to the services referred to in the event of concluding, surrendering and paying out, as well as providing intermediary services in the conclusion, surrendering and paying out of a life insurance contract, and of other investment-related insurance products, including: the insured amount and the relevant policy number. The criteria as set out is addressed in Article 8 paragraph 2 sub b:a service provider that is a life insurer can, identify the beneficiary of a policy and verify the identity after the business relationship has been established; in that case the identification and verification of identity will take place on or before the time of payment or on or before the time at which the beneficiary wishes to exercise his rights under the policy;	**The deficiency is addressed.** This Criterion was considered Not Met in the 4th round MER. Article 20 subsection 2e of the WMTF requires CDD information to be established in the event of concluding, surrendering and paying out, as well as providing intermediary services in the conclusion, surrendering and paying out of a life insurance contract, and of other investment-related insurance products, including: the insured amount and the relevant policy number. Criteria 10.12 is now **Met**.

R.10	PC	C.10.13	There are no measures for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.	(Changed provision) The definition for client (Article 1 paragraph 1 sub g) also extends to the person who pays the premium, as well as the beneficiary when concluding, commuting and paying out, as well as providing mediation in the conclusion, surrendering and paying out of a life insurance contract and other unit-linked insurance products (Article 1 paragraph 1 sub c5). In this regard the definition for beneficiary should also be taken into consideration (Article 1 paragraph 1 sub bb): a natural person, legal entity, or any other form of company which is not a legal entity or category of persons to whom benefits are paid under an insurance policy when/if an insured event covered by the policy occurs. Article 3 paragraph 1 and 2 state that a service provider takes measures to periodically identify and assess its risks of money laundering and terrorism financing, whereby the measures are proportionate to the nature and size of the service provider. When determining and assessing the risks referred to in the first paragraph, the service provider will in any case take into account the risk factors associated with the type of client, product, service, transaction and delivery channel and with countries or geographical areas. Service providers also takes into account the results of the national and sectoral risk analyses. As such in instances where the results of identifying and assessing risks entail a higher risk of ML or TF with regard to the beneficiary of a life insurance policy the provisions for enhanced due diligence as set forth in Article 14 of the WMTF will apply.	**The deficiency is not addressed.** This Criterion was considered Not Met in the 4th round MER. There are no measures for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. Criteria 10.13 remains **Not Met**.

R.10	PC	C.10.14	Met	(Unchanged provision) Article 8 paragraph 1 of the WMTF requires the identification and verification measures for the customer and beneficial owner to be conducted prior to entering into the business relationship or executing a non-recurrence transaction. Furthermore Article 8 paragraph 2 states that: notwithstanding the provisions of paragraph 1: a. a service provider verifies the identity of the client and the ultimate beneficial owner during the business relationship, if this is necessary in order not to disrupt the service and if there is little risk of money laundering or terrorist financing; in that case, the service provider verifies the identity as soon as possible after the first contact with the client; b. a service provider that is a life insurer, identifies the beneficiary of a policy and verifies identity after the business relationship has been established; in that case the identification and verification of identity will take place on or before the time of payment or on or before the time at which the beneficiary wishes to exercise his rights under the policy; c. a service provider that is a bank opens an account before the verification of the customer's identity has taken place, if it guarantees that this account cannot be used before the verification has taken place; d. a service provider who is a civil-law notary and/or junior civil-law notary verifies the identity of the client and that of the client's ultimate beneficial owner when identification is required. Article 8 paragraph3 WMTF states that if a service provider has reasonable suspicion that a client is involved in money laundering or terrorist financing, and the performance of the customer due diligence could lead to the client becoming aware of that suspicion, the service provider may terminate the customer due diligence. The service provider is obliged to report to FIU Suriname as referred to in Article 29. These stipulations were previously included in article 2a paragraph 1 and 2 of the WID Act.	This criterion was considered Met in the 4th round MER as no deficiency was cited. Article 8 sub section 2a requires a service provider to verify the identity of the client and the ultimate beneficial owner during the business relationship, if this is necessary in order not to disrupt the service and if there is little risk of money laundering or terrorist financing; in that case, the service provider verifies the identity as soon as possible after the first contact with the client. The provision complies with the requirements of the criterion. Criterion 10.14 remains **Met**.

R.10	PC	C.10.15	There are measures for the timing of verification, but they do not include appropriate risk management procedures.	(Changed provision) Article 2 and 3 of the WMTF requires FI's to adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification. Article 2 stipulates that service providers apply a risk-based program that includes the necessary policies, procedures and measures to comply with the rules laid down by or pursuant to this law regarding risk management, internal control measures, customer due diligence, record keeping and unusual transaction reporting to prevent money laundering and terrorism financing. In the explanatory notes clarity is given in Art 2 stating that the risk approach is introduced within this law and is the integral starting point for the design of the service provider's business operations aimed at preventing involvement in money laundering and terrorist financing. The general principles of this approach relate to the design and application of effective risk management. The business risk or business analysis should not be viewed as a static, one-time action, but as an ongoing liability. After all, risks are not static but dynamic and the service provider must therefore regularly update the analysis. This is usually periodic (time-bound), but also in case of major changes for the company, such as a change in the business or profit model, takeover(s), structural organizational adjustments or major external changes such as new or updated laws and regulations on the in the field of preventing and combating money laundering and terrorist financing, as a result of which adapted or newly introduced measures can be expected. Article 3 states that service providers should take measures to periodically identify and assess its risks of money laundering and terrorism financing, whereby the measures are proportionate to the nature and size of the service provider. Article 8pragraph 2 sub a of the WMTF allows the service provider to verify the identity of the client and the ultimate beneficial owner during the business relationship. But it also states that there should be little risk of ML or TF. This implies that the service provider should conduct some assessment of risk. Art 7 subparagraph 2a requires services providers to identify and verify the client's identity when applying CDD. Client as defined in the WMTF as: a natural person, legal person or legal arrangement. With regard to the requirement that FIs must adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification the articles 4 and 5 of the WMTF apply and state the following: Article 4	**The deficiency is addressed.** This Criterion was considered Not Met in the 4th round MER. Pursuant to Article 8 Sub section 2a of the WMTF, a service provider is permitted to enter into a business relationship prior to verification (see above c. 10.14).However, verification must occur before any transactions are carried out. Further, article 8 Subsection 2c of the WMTF states that a service provider that is a bank opens an account before the verification of the customer's identity has taken place, if it guarantees that this account cannot be used before the verification has taken place. The above requirements under the WMTF, that prohibit the utilization of the business relationship prior to verification, negate the need for the adoption of the risk management procedures under C.10.15. Criteria 10.15 is considered Not Applicable on the basis of the explanation provided above. . 1.

				1. A service provider shall have policies, procedures and measures in place to mitigate and effectively manage the money laundering and terrorist financing risks identified in accordance with Article 3 and the risks identified in the national risk assessment. Tightened measures will be taken to control and limit identified higher risks. 2. The policies, procedures and measures referred to in paragraph 1 are proportionate to the nature and size of the service provider's organization and activities and relate at least to compliance with the provisions in Chapter 1, paragraphs 1.2 and 1.3, Chapter 2, Sections 2.1 to 2.4, and Chapter 3, Section 3.2. 3. The policies, procedures and measures require the approval of senior management or those who determine the day-to-day policy of the service provider at the highest level. 4. A service provider ensures a systematic review of the policies, procedures and measures and, where necessary, adjusts them. 5. The supervisors shall lay down further rules regarding the identification, assessment, management and mitigation of the risks of money laundering and terrorist financing. Article 5 1. A service provider shall establish an independent and effective compliance function in accordance with the type and size of the service provider's organization and activities. 2 The compliance function referred to in paragraph 1 is responsible for developing compliance programs to prevent and combat money laundering and terrorist financing. 3. The supervisors lay down further rules regarding the compliance programme. Additionally, the Explanatory Notes highlight the following: The risk approach is introduced with this law and is the integral starting point for the design of the service provider's business operations aimed at preventing involvement in money laundering and terrorist financing. The general principles of this approach relate to the design and application of effective risk management. This primarily concerns the identification and analysis of the risks of money laundering and terrorist financing as they apply to the service providers, taking into account the nature and size of its organisation, professional activities and given its clientele, products and services offered, geographical exposure and the delivery channels used (the inherent risk factors). The next step is the assessment by the service provider of the measures taken to limit, manage or eliminate the risks, effectively mitigating the identified inherent risks (or: vulnerabilities). The ultimately determined risk will then consist of a residual risk concept (total residual risk) for which	

				specific measures must be taken to mitigate this by means of the necessary adjusted or implemented policy, procedures and control measures. Where higher risks have been identified, stricter measures must be taken, while lower risks - within the limits set by this law - can be tackled with simplified measures. The required procedures may relate to the administrative organization and internal control of the service provider, recruitment, change of position, background, training, informing and retraining of the personnel concerned, applying customer due diligence, recording data and information, the internal decision-making process for reporting and periodic evaluation of the effectiveness of those procedures and measures. An important elaboration of the approach consists of the obligation for the service providers to carry out risk-based customer due diligence (article 10), as well as the monitoring of transactions (article 7 paragraph 2 sub d), and this may also relate to the development of employee training and other additional controls. Bearing in mind that the risk assessment can also lead to a service provider coming to the conclusion that insufficient control measures are possible and that certain risks must therefore be avoided entirely. Art 8 of the WMTF should be read in conjunction with Art 7 of the WMTF, were latter states the risk management procedures for FIs. Art 8 sub 2c specifically states that FIs may utilize the business relationship prior to the verification, meaning open a bank account. The explicit condition for the FI according to aforementioned Article is that the FI has to guarantee that the account cannot be used before the verification has taken place.	

R.10	PC	C.10.16	Met	(Unchanged provision) Article 7 paragraph 2 sub d requires for continuously monitoring of the business relationship and the transactions carried out during the term of this relationship, in order to ensure that they correspond to the knowledge that the service provider has of the customer and his risk profile, including, if necessary, an investigation into the origin of the resources used in the business relationship or transaction; This was previously included in art 2 sub 1d of the WID. Pursuant to section 2 I. of the 2016 CBvS-AML/CFT Directive, FIs should continue to apply CDD-procedures to new and existing customers, adjusting the scope of the measures on a risk sensitivity basis according to the type of customer, the business relationship or the transaction, including ongoing monitoring. FIs should closely examine all transactions performed during their business relationship to be sure that the transactions carried out are in line with the information that the institution has about the business, the risk profile, and the origin of the customer's funds.	This criterion was considered Met in the 4th round MER as no deficiency was cited. Article 7 sub section 2d of the WID Act requires ongoing monitoring to be conducted on customers. Further, pursuant to section 2 I. of the 2016 CBvS Directive, FIs should continue to apply CDD-procedures to new and existing customers, adjusting the scope of the measures on a risk sensitivity basis according to the type of customer, the business relationship, or the transaction, including ongoing monitoring. Criterion 10.16 remains **Met.**
R.10	PC	C.10.17	Met	(Unchanged provision) Article 14 paragraph 1 of the WMTF requires that service providers perform enhanced customer due diligence if and to the extent that a business relationship or transaction – based on an adequate risk assessment – entails a higher risk of money laundering or terrorist financing. The enhanced customer due diligence measures applied by the service providers must adequately manage and limit the identified higher risks. This was previously in article 4 sub 1 of the WID Act. Section 2 I. of the 2016 CBvS-AML/CFT Directive requires FIs to perform CDD and enhanced due diligence measures where higher ML/TF risk have been identified. FIs should apply CDD-procedures to new and existing customers, adjusting the scope of the measures on a risk sensitivity basis according to the type of customer, the business relationship or the transaction. The enhanced CDD procedures should be applied both before and during the business relationship or transaction. Also paragraph VI (Complex and large-scale transactions and activities) and paragraph VII (Foreign business relationships in high-risk countries).	This criterion was considered Met in the 4th round MER as no deficiency was cited. Article 14 of the WMTF Act and section 2 I. of the 2016 CBvS Directive (Pg.8-9)) requires FIs to perform enhanced due diligence measures where higher ML/TF risk have been identified. The above provision complies with the requirements of the criterion. Criterion 10.17 remains **Met.**
R.10	PC	C.10.18	There are no specific measures for SDD where lower risks are identified.	(Changed provision) With regard to specific measures for SDD where lower risks are identified article 13 paragraph 1 of the WMTF states that notwithstanding Article 7, based on an adequate assessment of the risks, a service provider may conduct a simplified customer due	**This deficiency is addressed.** This Criterion was considered Not Met in the 4th round MER. Suriname has put in place, measures under Article 13 of the WMTF, that require FIs may only be permitted to apply SDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the financial institution. Pursuant to Article 13 sub

				diligence if a business relationship or transaction by its very nature entails a low risk of money laundering or terrorist financing. The simplified measures should be proportionate to the lower risk factors. In addition, Article 13 states that simplified customer due diligence can be applied: a. with regard to the following clients: 1° the Surinamese government and other legal persons established under public law in Suriname; 2° public limited companies of which all shares are held by the State. b. if they carry out a transaction or enter into a business relationship related to: 1° a life insurance contract of which the premium due on an annual basis or of which the amount of the single premium does not exceed the amount to be determined by State Decree; 2° a pension or comparable scheme that aims to provide an old-age provision to an employee, whereby the contributions for the benefit of the pension provisions are made by means of deduction from the employee's salary and whereby the employee is not allowed to use his pension ensuing from the pension scheme to transfer, pledge or transfer rights to third parties as security; 3° ultimate beneficial owners in designated non-financial service provider accounts that are used exclusively for holding funds of third parties, provided these service providers are subject to regulations for the prevention and control of money laundering and terrorism financing that comply with the internationally accepted standards for the prevention and combating of money laundering and terrorist financing, and are subject to effective supervision with regard to compliance with these standards; 4° a financial product or financial service that includes predefined and provides limited services to certain groups or types of clients with an aim to promote financial inclusion. 3. The service provider demonstrably collects sufficient data on the understanding that the service provider must make every effort to demonstrate that there is a low risk. 4. The provisions of paragraph 1 do not apply if the client, business relationship or transaction entails a higher risk of money laundering or terrorist financing or if there are indications that the client is involved in money laundering or terrorist financing.	section 4 of the WMTF, the SDD measures permitted under Article 13 sub section 1 of the WMTF do not apply if the client, business relationship or transaction entails a higher risk of money laundering or terrorist financing or if there are indications that the client is involved in money laundering or terrorist financing. Criterion 10.18 is now **Met.**

R.10	PC	C.10.19(b)	The requirement for making a disclosure to the FIUS is limited to when the service provider (FIs) cannot perform CDD after the business relationship has commenced.	(Changed Provision) Article 9 of the WMTF states that without prejudice to article 8 paragraph 2, a service provider is prohibited from entering into a business relationship or carrying out a transaction if it has not performed customer due diligence, if it is unable to perform customer due diligence or if the customer due diligence has not led to the result envisaged in Article 7. In the explanatory notes clarification is given in paragraph 1 stating that , the prohibition set out in Article 8 paragraph 2 is given a broader scope of application, namely that no business relationship can be entered into or a transaction can be carried out if the service provider has not conducted customer due diligence, if it is unable to perform customer due diligence (e.g. due to a reluctant attitude on the part of the client) or if the client due diligence has not led to the result intended by Article 7, namely obtaining the most complete possible picture of the client and the ultimate beneficial owner in the context of preventing and combating fraud. money laundering and terrorism financing. 2. If, after entering into a business relationship, a service provider can no longer comply with the provisions of Article 7, it will immediately terminate this business relationship and make a notification as referred to in Article 29.	**The deficiency is not addressed.** This Criterion was considered Mostly Met in the 4th round MER. Pursuant to Article 9 paragraph 1 of the WMTF, a service provider is prohibited from entering into a business relationship or carrying out a transaction if it has not performed customer due diligence, if it is unable to perform customer due diligence or if the customer due diligence has not led to the result envisaged in Article 7 of the WMTF. Further, Article 9 paragraph 2 of the WMTF, states, if after entering into a business relationship, a service provider can no longer comply with the provisions of Article 7, it will immediately terminate this business relationship and make a notification as referred to in Article 29 (which deals with the reporting obligations). However, there exists no obligation for FIs to consider filing an STR in relation to the customer for failing to provide the relevant CDD. Criterion 10.19 remains **Mostly Met.**
R.10	PC	C.10.20	There are no measures for a situation where performing CDD will tip off the customer.	(Changed provision) According to Article 8 paragraph 3 of the WMTF if a service provider has reasonable suspicion that a client is involved in money laundering or terrorist financing, and the performance of the customer due diligence could lead to the client becoming aware of that suspicion, the service provider may terminate the customer due diligence. The service provider is obliged to report to FIU Suriname as referred to in Article 29. Sections 2 X. (Exclusion of Liability) of the 2016 CBvS-AML/CFT Directive also notes that FIs and their management and staff may not disclose to the customer or third parties that information has been provided to the FIU or that an investigation into ML activities is being carried out, unless the FIU desires otherwise.	This criterion was considered Met in the 4th round MER as no deficiency was cited. According to Article 8 paragraph 3 of the WMTF if a service provider has reasonable suspicion that a client is involved in money laundering or terrorist financing, and the performance of the customer due diligence could lead to the client becoming aware of that suspicion, the service provider may terminate the customer due diligence. The service provider is obliged to report to FIU Suriname as referred to in Article 29. Further, Sections 2 X. (Exclusion of Liability) of the 2016 CBvS-AML/CFT Directive also notes that FIs and their management and staff may not disclose to the customer or third parties that information has been provided to the FIU or that an investigation into ML activities is being carried out, unless the FIU desires otherwise. Criterion 10.20 remains **Met.**
R.10	**Overall Conclusion**	**R.10 is remains partially compliant on the basis that moderate shortcomings still exist within Suriname's AML/CFT framework.** Whilst most of the CDD measures are in place in Suriname, deficiencies still exist in current AML/CFT legislative framework. Suriname has no provision that specify the threshold of USD/EUR 15,000 for carrying out occasional transactions by FIs which is considered a minor deficiency. In the insurance context, there is no legislation that requires the FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. These deficiencies are not weighted heavily based on Suriname's risk and context and the size of the insurance sector**.** With respect to CDD measures, there are no measures with respect to: (1) identification and verification requirements for legal arrangements (including their beneficial owners); (2) understanding the nature			

		of the client's business when performing identification and verification procedures for a legal entity or any other form of business which is not a legal entity; (3) obtaining information on the powers that regulate and bind legal persons or arrangements; (4) regarding a legal entity governed by public law and religious organisation, in addition to the same deficiency as local or foreign entities, there is no requirement for obtaining proof of existence; (5) there exists no obligation for FIs to consider filing an STR in relation to the customer for failing to provide the relevant CDD. These deficiencies are weighted heavily as some relate to higher risk areas such as identification and verification of beneficial ownership and proof of existence. **Recommendation 10 is re-rated partially compliant.** **Please revise text according to the clarifications and citation given in the sub criteria of Recommendation 10 with regard to CDD measures for legal entities and legal arrangements as well as risk managements procedures are clearly stipulated in the WMTF. Rec 10 should be upgraded to LC given the fact that the deficiency as indicated in the overall conclusion is addressed in the WMTF. As also referred by the expert in the column Analysis and Conclusion the deficiency to cover a legal entity or any other form of business arrangement that is not a legal entity is addressed with the amendment of Article 11 paragraph 1 sub sections a, b, c, and d of the WMTF.** **Experts Response:** **The Experts have reviewed the additional information submitted by the Suriname Authorities and maintains the view that those provisions cited do not address the deficiencies that were outlined in the above conclusion for R.10. As such, R.10 remains Partially Compliant.**			
R.12	PC	C.12.1	Met	(Changed provision) Articles 2, 3 and 4 of the WMTF regarding Risk management. Article 2: To prevent money laundering and terrorism financing, a service provider applies a risk-based program that includes the necessary policies, procedures and measures to comply with the rules laid down by or pursuant to this law regarding risk management, internal control measures, customer due diligence, record keeping and unusual transaction reporting. Article 3: Paragraph 1. A service provider takes measures to periodically identify and assess its risks of money laundering and terrorism financing, whereby the measures are proportionate to the nature and size of the service provider. Paragraph 2. When determining and assessing the risks referred to in the first paragraph, the service provider will in any case take into account the risk factors associated with the type of client, product, service, transaction and delivery channel and with countries or geographical areas. Service providers also takes into account the results of the national and sectoral risk analyses. Paragraph 3. A service provider takes adequate measures to identify and assess the risks of money laundering and the financing of terrorism that may arise from the development and use of new technologies, products and commercial practices, including new service delivery mechanisms. This risk assessment will be performed prior to the introduction or use of such technologies, products and commercial practices. Paragraph4. A service provider shall record the assessment process and the results of identifying and assessing its risks, keep it up to date and provide these results to the supervisory authority upon request.	This criterion was considered Met in the 4th round MER as no deficiency was cited. In relation to foreign PEPs, in addition to performing CDD measures required under R.10, FIs are required to: **(a) (Met)** put in place adequate policies and procedures to determine whether a customer, a potential customer or an ultimate beneficial owner is a PEP. (See articles 16 subsection 1 of the WMTF Act and section 2 I. of the 2016 CBvS Directive (Pg.13)). **(b) (Met)** obtain executive or senior management approval before establishing a business relationship (or continuing, for existing customers) or performing a transaction with a PEP (See articles 16 subsections 3b of the WMTF Act and section 2 I. of the 2016 CBvS Directive (Pg.13)). **(c) (Met)** establish the source of wealth and funds of customers and ultimate beneficial owners regarded as PEP. (See articles 16 subsection 3c of the WMTF Act and section 2 I. of the 2016 CBvS Directive (Pg.13)). **(d) (Met)** conduct enhanced ongoing monitoring of the PEP business relationships (See 16 3d of the WMTF Act,14 subsection 3g of the WMTF Act and section 2 I. of the 2016 CBvS Directive (Pg.8-9)). Criterion 12.1 remains **Met**.

				Article 4: Paragraph 1. A service provider shall have policies, procedures and measures in place to mitigate and effectively manage the money laundering and terrorism financing risks identified in accordance with Article 3 and the risks identified in the national risk assessment. Tightened measures will be taken to control and limit identified higher risks. Paragraph 2. The policies, procedures and measures referred to in paragraph 1 are proportionate to the nature and size of the service provider's organization and activities and relate at least to compliance with the provisions in Chapter 1, paragraphs 1.2 and 1.3, Chapter 2, Sections 2.1 to 2.4, and Chapter 3, Section 3.2. Paragraph 3. The policies, procedures and measures require the approval of senior management or those who determine the day-to-day policy of the service provider at the highest level. Paragraph 4. A service provider ensures a systematic review of the policies, procedures and measures and, where necessary, adjusts them. Paragraph 5. The supervisors shall lay down further rules regarding the identification, assessment, management and mitigation of the risks of money laundering and terrorism financing. This article was previously 9 of the WID Criteria 12.1 (a) Pursuant to Article 16 paragraph 1 of the WMTF service providers are required to put in place adequate policies and procedures to determine whether a client, a potential client or an ultimate beneficial owner is a PEP. Criteria 12.1 (b) Article 16 paragraph 3 sub b states that service providers are required to obtain executive or senior management approval before establishing a business relationship (or continuing, for existing customers) or performing a transaction with a PEP. Criteria 12.1 (c) Article 16 paragraph 3 sub c requires service providers to establish the source of wealth and funds of clients and beneficial owners regarded as PEPS. Criteria 12.1 (d) Article 16 paragraph 3 sub d requires service providers to conduct enhanced ongoing monitoring of the PEP business relationship. Section 2 I. (paragraph Politically Exposed Persons, page 13) of the 2016 CBvS-AML/CFT Directive provides guidance in regard to PEP's.	

				(a) FIs have in place adequate policies and procedures to determine whether a customer, a potential customer or an ultimate beneficial owner is a PEP. (b) FIs should obtain executive or senior management approval before establishing a business relationship (or continuing, for existing customers) or performing a transaction with a PEP. (c) FIs should establish the source of wealth and funds of customers and ultimate beneficial owners regarded as PEP. (d) FIs should conduct enhanced ongoing monitoring of the PEP business relationships (Section 2 I. of the CBvS Directive (Page 8-9))	
R.12	PC	C.12.2	Suriname's current legislation does not define or make any reference to the domestic PEPs or persons who have been entrusted with a prominent function by an international organization and their immediate family members and close associates. There are no defined CDD measures for the domestic PEPs or persons who have been entrusted with a prominent function by an international organisation.	(Changed provision) According to Article 1 paragraph 1 sub x of the WMTF a PEP is defined as a person who holds or has held a prominent public position abroad or domestically, or who holds or has held a prominent position or position within an international organization. Therefore, a definition of domestic PEP is now included in the WMTF and addresses the main deficiency in recommendation 12. Based on this definition the following articles regarding PEPs apply to both domestic and foreign PEPs. Criteria 12.2 (a) Pursuant to Article 16 paragraph 1 WMTF service providers are required to put in place adequate policies and procedures to determine whether a client, a potential client or an ultimate beneficial owner is a PEP. Furthermore Article 16 paragraph 3 sub a requires service providers to determine whether the client or ultimate beneficial owner is a politically exposed person through appropriate risk assessment. Criteria 12.2 (b) Article 14 paragraph 3 sub g is applicable with regard to PEPs as this article requires service providers to conduct enhanced due diligence. Reference is also made to the text submitted for criteria 12.1 b to d. Criteria 12.2 © Article 16 paragraph 3 sub c states that service providers should take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs Criteria 12.2 d Subsequently Article 16 paragraph 4 states that EDD also extends to the immediate family members and close relatives of the identified PEP	**This deficiency is addressed.** This Criterion was considered Not Met in the 4th round MER. Article 1 paragraph 1 sub x of the WMTF was amended to define a Politically Exposed Person as a person who holds or has held a prominent public position aboard or domestically or holds or has held a prominent function or position within an international organisation. This amendment by way of the WMTF now provides for CDD measures(Article 16, para 3) and enhanced ongoing monitoring (Article 16 sub section 3 (d), Article 14 sub section 3 (g) for domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, as well as the requirement to obtain senior management approval to establish or continue such relationships (Article 16 sub section 3 (b) and the requirement to take reasonable steps to determine source of funds and source of wealth (sub section 3 (c)). Criterion 12.2 is now **Met.**

R.12	PC	C.12.3	There are no defined CDD measures for the domestic PEPs and their family members or close associates, neither are there measures for persons who have been entrusted with a prominent function by an international organization.	(Changed provision) Criteria 12.3 Subsequently Article 16 paragraph 4 states that EDD also extends to the immediate family members and close relatives of the identified PEP. Reference is also made to the submitted text for criteria 12.1 and 12.2	**This deficiency is addressed.** This Criterion was considered Partly Met in the 4th round MER. Article 16 sub section 4 of the WMTF Act notes that the provisions for PEPs under Article 16 apply to family members and close relatives of the politically exposed person. The application of this provision is clarified in the Explanatory Memorandum for Article 16 whereby the requirements for PEPs also apply to the close associates of the PEP, as required under Criterion 12.3. Criterion 12.3 is **Met.**

R.12	PC	C.12.4	There is no requirement in Suriname's legislation that requires FIs to determine whether the beneficiaries and/or where required, the beneficial owner of a beneficiary of a life insurance policy is a domestic PEP.	(Changed provision) Criteria 12.4 Reference is made to Article 8 paragraph 2 sub b: a service provider that is a life insurer can, identify the beneficiary of a policy and verify the identity after the business relationship has been established; in that case the identification and verification of identity will take place on or before the time of payment or on or before the time at which the beneficiary wishes to exercise his rights under the policy. Furthermore, Art icle16 paragraph 1- 4 requires the following: 1 The Service provider has an adequate policy and uses special procedures to determine whether a client, a potential client or an ultimate beneficial owner is a politically exposed person. 2. If the client or the ultimate beneficial owner becomes or appears to be a politically exposed person during the business relationship, the service provider will take the measures referred to in paragraph 3 under b, c and d without delay after this has become apparent. 3. Service providers are obliged with regard to the politically exposed person, as a client or ultimate beneficial owner, in addition to the usual client due diligence as referred to in Article 7, also: a. determines through appropriate risk assessment whether the client or ultimate beneficial owner is a politically exposed person; b. obtain approval from senior management for the establishment (or continuation for existing customers) of those business relationships; c. takes reasonable steps to establish the origin of assets and assets, and d. to exercise stricter supervision on the business relationship on an ongoing basis. 4. This article applies mutatis mutandis to family members and close relatives of a politically exposed person.	**This deficiency is partly met.** This Criterion was considered Partly Met in the 4th round MER. Article 8 sub section 2 sub b of the WMTF requires that a service provider that is a life insurer, identify the beneficiary of a policy and verify the identity after the business relationship has been established. In such cases the identification and verification of identity will take place on or before the time of payment; or on or before the time at which the beneficiary wishes to exercise his rights under the policy. There is no requirement for senior management involvement before paying out in cases where the beneficiaries have been identified as PEPs. Where higher risks are identified, there is no requirement for FIs to consider making a suspicious transaction report. Criterion 12.4 is now **Mostly Met.**

R.12	**Overall Conclusion**	The deficiencies noted in the 4th round MER have been largely addressed with the amendments made within the WMTF. There is, however, no requirement for senior management involvement before paying out in cases where the beneficiaries have been identified as PEPs and no obligation to consider making a STR. Due to the limited risks, the issues relating to life insurance are given minimal weighting. On the basis that the deficiencies outlined in the 4th Round MER have now been largely addressed, with minor shortcomings remaining, R.12 is upgraded from **partially compliant to largely compliant.**			
R.13	PC	C.13.1(a)	There are no specific measures to be adopted for other similar relationships, apart from correspondent banking relationships, to include securities transactions or funds transfers whether for the cross border FIs as principal or for its customers	(Changed provision) Criteria 13.1 (a) Reference is made to Article 17 paragraph 1 sub a of the WMTF requiring that service providers who intend to enter into a correspondent bank or similar relationship shall ensure they collect sufficient information about the respondent institution to obtain a full picture of the nature of its business activities and to establish the reputation of the respondent institution and the quality of supervision exercised over that institution, including information about any investigations into money laundering and terrorist financing or measures taken as part of supervision. The requirement is now also applicable to similar relationships. The CBvS-AMLCFT Directive (Section 2 paragraph II. Cross-border correspondent banking) provides measures to FIs involved in correspondent banking in addition to the normal CDD-procedures: a. to gather sufficient information about the respondent institution so as to fully assess the nature of its business activities and its reputation on the basis of the available information, as well as the quality of its supervision, including the question as to whether the institution concerned has been involved in an investigation into money laundering or the financing of terrorism, or has been subjected to regulatory action;	**This deficiency is addressed.** This criterion was considered Partly Met in the 4th round MER. Article 17 section 1a of the WMTF Act requires that a service provider who intends to enter into a correspondent bank or similar relationship shall ensure that: a. it collects sufficient information about the respondent institution to obtain a full picture of the nature of its business activities and to establish the reputation of the respondent institution and the quality of supervision exercised over that institution, including information about any investigations into money laundering and terrorist financing or measures taken as part of supervision. Criterion 13.1(a) is now **Met**.
R.13	PC	C.13.1(b)	There are no defined measures to assess the adequacy of the respondent institutions' AML/CFT systems, procedures and controls.	(Changed provision) Criteria 13.1 (b) Article 17 paragraph 1 sub b states that service providers should assess the respondent institution's procedures and measures to prevent money laundering and terrorist financing and ascertains that these are adequate and effective. The CBvS-AMLCFT Directive (Section 2 paragraph II. Cross-border correspondent banking) provides measures to FIs involved in correspondent banking in addition to the normal CDD-procedures: to assess the respondent institution's internal anti-money laundering and terrorist financing controls, at determine whether they are adequate and effective;	**This deficiency is addressed.** This criterion was considered Not Met in the 4th round MER. The deficiencies noted in the 4th round MER have now been addressed. Article 17 section 1b of the WMTF Act requires that a service provider who intends to enter into a correspondent bank or similar relationship shall ensure that: b. it assesses the respondent institution's procedures and measures to prevent money laundering and terrorist financing and ascertains that these are adequate and effective. Criteria 13.1(b) is now **Met.**

R.13	PC	C.13.1(c)	Met	(Unchanged provision) Criteria 13.1 c Pursuant to Article 17 paragraph 2 requires that service providers only enter into a new correspondent bank or similar relationship after a decision to that effect has been made by the persons charged with the overall management of the service provider. This was previously in article 13 section 2 of the WID Act. The CBvS-AMLCFT Directive (Section 2 paragraph II. Cross-border correspondent banking) provides measures to FIs involved in correspondent banking in addition to the normal CDD-procedures: (c) to obtain approval from the Senior management before establishing new correspondent-bank relationships;	This criterion was considered met in the 4th round MER as no deficiency was cited. Article 17 section 2 of the WMTF Act states that a service provider enters into a new correspondent bank or similar relationship only after a decision to that effect has been made by the persons charged with the overall management of the service provider. Persons charged with overall management constitute senior management. Criteria 13.1(c) remains **Met**.
R.13	PC	C.13.1(d)	Met	(Unchanged provision) Criteria 13.1 (d) According to Article 17 paragraph 1 sub c service providers are required to ascertain that the responsibilities of both institutions in the field of preventing and combating money laundering and terrorist financing are laid down in writing. This was previously in article 13 section 1c of the WID Act. The CBvS-AMLCFT Directive (Section 2 paragraph II. Cross-border correspondent banking) provides measures to FIs involved in correspondent banking in addition to the normal CDD-procedures: (d) to document the respective responsibilities of each institution;	Criteria 13.1(c) (met). This criterion was considered met in the 4th round MER as no deficiency was cited. Article 17 section 1c of the WMTF Act states that a service provider who intends to enter into a correspondent bank or similar relationship shall ensure that the responsibilities of both institutions in the field of preventing and combating money laundering and terrorist financing are laid down in writing. Criterion 13.1(c) remains **Met.**
R.13	PC	C.13.2	Met	(Unchanged provision) Criteria 13.2 (a and b) Article 17 paragraph 3 of the WMTF states that if a correspondent banking relationship involves the use of transit accounts, the correspondent bank shall satisfy itself that the respondent bank has identified its clients who have direct access to those transit accounts, including their ultimate beneficial owners, verified their identity and has continued control over the business relationship with these clients in accordance with internationally accepted standards for identification and identity verification. The correspondent bank furthermore ascertains that the respondent bank is able to provide the bank with all relevant client due diligence data on request. This article was previously article 13 section 3 of the WID Act. The 2016 CBvS-AMLCFT Directive (Section 2 paragraph II. Cross-border correspondent banking) FIs are required to satisfy themselves with respect to "payable-through accounts," to be satisfied that the respondent institution has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent,	This criterion was considered Met in the 4th round MER as no deficiency was cited. Pursuant to Article 17 section 3 of the WMTF Act, a service provider who intends to enter into a correspondent bank or similar relationship shall ensure that If a correspondent banking relationship involves the use of transit accounts, the correspondent bank shall satisfy itself that the respondent bank has identified its clients who have direct access to those transit accounts, including their ultimate beneficial owners, verified their identity and has continued control over the business relationship with these clients in accordance with internationally accepted standards for identification and identity verification. The correspondent bank furthermore ascertains that the respondent bank is able to provide the bank with all relevant client due diligence data on request for the application of the first sentence, the term 'transit account' shall be understood to mean a correspondent account held by an involved bank with a bank to which third parties have direct access for the execution of transactions on their own behalf. Further, pursuant to section 2 II. of the 2016 CBvS Directive FIs are required to satisfy themselves with respect to "payable-through accounts," to be satisfied that the

				that the customers are subject to on-going CDD-procedures, and that it is able to provide the relevant customer identification data to the correspondent institution upon request.	respondent institution has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent, that the customers are subject to on-going CDD-procedures, and that it is able to provide the relevant customer identification data to the correspondent institution upon request. Criterion 13.2 remains **Met**.
R.13	PC	C.13.3	Met	(Unchanged provision) Criteria 13.3 Pursuant to Article 17 paragraph 4 of the WMTF a bank is prohibited from entering into or maintaining a correspondent banking relationship with a shell bank. Subsequently Article 17 paragraph 5 requires that banks ensure that financial service providers established outside Suriname with whom they enter into or maintain a correspondent banking relationship do not allow their accounts to be used by shell banks. If a situation arises as referred to in the first sentence, the relevant bank will immediately terminate the correspondent banking relationship and notify FIU Suriname of this. This was previously in article 14 section 1 of the WID Act. The 2016 CBvS-AML/CFT Directive (Section 2 paragraph II. Cross-Border Correspondent Banking) FIs are, nevertheless, not permitted to enter into correspondent banking relations with so-called "Shell Banks." A "Shell Bank" is a financial institution established outside Suriname, that has no physical presence in the country of its establishment and is not subject to effective consolidated supervision. Special attention must also be paid to correspondent services to FIs that are established in jurisdictions where AML and TF regulations are insufficient, as ascertained by FATF and its affiliated organizations. Financial institutions which maintain a correspondent banking relationship should discuss and exchange and update their ML and TF policy at set times to avoid miscommunications (prohibition of relationships with shell banks is still in effect).	This criterion was considered Met in the 4th round MER as no deficiency was cited. Pursuant to article 17 section 4 of the WMTF Act states that a bank is prohibited from entering or maintaining a correspondent banking relationship with a shell bank. Pursuant to article 17 section 5 of the WMTF Act, the banks are also expected to satisfy themselves that the financial service providers that have their registered office outside of Suriname with which they enter into or maintain a correspondent banking relationship do not permit their accounts to be used by shell banks. If a situation occurs as referred to in the first sentence, the relevant bank will immediately terminate the correspondent banking relationship and notify FIU Suriname of this. Section 2 II. of the 2016 CBvS Directive (Pg.14) also notes that the FIs are not permitted to enter into correspondent banking relationships with shell banks. Criterion 13.3 remains **Met**.
R.13	**Overall Conclusion**	**R.13 is upgraded from PC to C on the basis that the deficiencies outlined under Criteria 13.1(a) and 13.1(b) of the 4th Round MER have now been addressed with the enactment of the WMTF.**			

R.21	PC	C.21.1	FIs and their directors are not protected by law from both criminal and civil liability when they disclose information related to TF.	(Changed provision) Criteria 21.1 According to Article 36 of the WMTF service providers, their directors and employees and their employees shall not be held criminally or civilly liable for the violation of restrictions on disclosure of information imposed by contract or by any statutory provision if they raise their suspicions of money laundering or related designated criminal offenses or financing of report terrorism, insider dealing and market manipulation to FIU Suriname. Furthermore Article 37 paragraph 1 and 2 state that: 1. The person who has made a report pursuant to Article 29 in good faith, or who has provided data or information to FIU Suriname pursuant to Articles 30 paragraph 1 and 31 paragraph 1 and 2, respectively, is not liable for damage suffered by a third party as a result. 2. Paragraph 1 applies mutatis mutandis to persons who work for the service provider and who have provided data or information in accordance with articles 29 paragraph 4, 30 paragraph 1 and 31 paragraph 1 and 2 and those who have contributed.	**This deficiency is addressed.** Article 36 of the recently enacted WMTF includes provisions that protect service providers, their directors and their employees, from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by statutory provisions. These provisions apply to the reporting of suspicions of money laundering, or related designated criminal offences or financing of terrorism, insider dealing and market manipulation, to FIU Suriname. Article 37 of the WMTF stipulates that individuals who make disclosures in good faith regarding suspicious activities related to money laundering or terrorist financing are protected from liability for any damage incurred by a third party as a direct consequence of their disclosure. **Criterion C.21.1 is Met.**

R.21	PC	C.21.2	Met	(Unchanged provision) Criteria 12 2 Article 45 paragraph 1 of the WMTF stipulates that data and information provided or received pursuant to the provisions of or pursuant to this Act are confidential. Anyone who provides or receives such data or information, including the person who makes a report pursuant to Article 29, paragraph 1, is obliged to keep it confidential. This requirement is the same as the requirement under article 25 of the MOT Act. Also the 2016 CBvS-AML/CFT Directive is still in effect. Paragraph X (Exclusion of liability) notes that FI's and their management and staff may not disclose to the customer or any other party that information has been provided to the FIU.	**Criterion 21.2 remains Met:** In accordance with Article 45, Paragraph 1 of the WMTF, any data or information provided or shared in relation to the Act is considered confidential. Furthermore, the Act states that anyone who provide or receive such data or information, including those who report an unusual transaction, are obligated to maintain its confidentiality. Criterion 21.2 remains **Met**.
R.21	**Overall Conclusion**	Suriname has taken significant steps through the passage of the WMTF, which include provisions aimed at safeguarding service providers, their directors and their employees, from both criminal and civil liability for breach of any restriction on disclosure of information (including those related to TF) imposed by contract or by statutory provisions. Additionally, the WMTF designates information shared under the Act as confidential. **On this basis, Suriname is re-rated as Compliant with R.21.**			

R.22	PC	C.22.1	The deficiencies identified in respect of CDD measures, record keeping, PEPs, ML/TF risks assessment and mitigating controls against new technologies, VA/VASPs and reliance on third parties, equally apply to DNFBPs	(Changed Provision) Subsequent to Article 7 paragraph 1 all service providers (including DNFBPs) are obligated to conduct customer due diligence in order to prevent and combat money laundering and terrorism financing. Paragraph 2 of the same article describes the requirements for CDD. Article 3 sub 3 also requires that DNFBPs take adequate measures to identify and assess the risks of money laundering and the financing of terrorism that may arise from the development and use of new technologies, products and commercial practices, including new service delivery mechanisms. This risk assessment will be performed prior to the introduction or use of such technologies, products and commercial practices. Text should be revised as well as rating according to Suriname's feedback regarding Criteria 10 as well as the conclusion of the overall Recommendation 10. Article 12 paragraph 1 refers to reliance on a third parties. Article 1 paragraph 1 sub b defines services as financial, non-financial or virtual asset services. Furthermore, a description for non-financial services is given in Article 1 paragraph 1 sub d stating the following: the professional or commercial performance, in or from Suriname, of one or more of the following activities for or on behalf of a client: 1. setting up and checking accounts and administrations, as an external chartered accountant, external accountant administration, consultant or a comparable professional; 2. giving advice or providing assistance as a lawyer, civil-law notary or junior civil-law notary, accountant, tax adviser or as an expert in the legal, tax or administrative field, or in the exercise of a similar legal profession or business, independently perform independent activities in connection with: a. the purchase and sale of immovable property; b. managing money, securities, coins, currency notes, precious metals, gemstones or other assets; c. managing bank, savings or securities accounts; d. establishing, operating or managing companies, legal persons or similar entities; e. the purchase, sale or takeover of companies; f. organizing contributions for the establishment, operation or management of companies. g. providing a registered office, business address, correspondence or administrative address; h. acting as a nominated shareholder or arranging for other persons to act as such. 3. trading in or mediating in the purchase and sale of immovable property, vehicles, ships, aircraft, works of art, antiques, and the rights to which these properties are subject;	**Criterion 22.1 is re-rated as partly met.** DNFPs fall under the WMTF and are classified as non-financial and virtual asset service providers (Article 1 a). As such, they are obligated to adhere to CDD requirements specified under the Act (Article 7 para. 1). The CDD measures outlined in the Act did not outline any de minimis threshold. The deficiency identified in the 4th Round MER is related to the use of a de minimis threshold of US$5,000 by game of chance providers when implementing CDD measures. This threshold exceeds the recommended limit of USD/EUR 3,000 (see Category H of the SDIUT) as advised by FATF. However, it is important to note that although the SDIUT remains in effect, this deficiency has been considered addressed. The expert took into consideration the fact that a de minimis threshold is not included in the WMTF. Furthermore, the expert also considered the fact that the WMTF is a legally binding law approved by the National Assembly, the highest institution in Suriname, and ratified by the President. Therefore, the WMTF takes precedence over any State decree(s) (including the SDUIT). R.10 has a cascading effect on this criterion. Under this round of rerating, R.10 remains Partially Compliant, which impacts the rating for C22.1. In coming to the partly met rating for C.22.1, the expert took into consideration that not all the measures outlined in R.10 would apply to DNFBPS (eg.C.10.12 and C.10.13). For a detailed review of the deficiencies in R.10, please refer to the re-rating assessment for this Recommendation. The identified deficiencies in R.10 were deemed substantial and had an impact on the rating for C.22.1. Criterion C.22.1 remains **Partly Met.**

				4. trading in gold and other precious metals and precious stones, involving financial transactions equal to or higher than an amount to be determined by state decree; 5. dealing in motor vehicles, involving financial transactions equal to or higher than an amount to be determined by state decree; 6. offering games of chance, involving financial transactions equal to or higher than an amount to be determined by state decree; e. Virtual asset services: the professional or commercial performance in or from Suriname of one or more of the following activities for or on behalf of a client: 1. exchange between virtual assets and fiat currencies; 2. exchange between one or more others forms of convertible virtual assets; 3. transfer of virtual assets, by carrying out a transaction, where virtual assets moved from one virtual asset address or account to another; 4. custody and/or administration of virtual assets or instruments under control enabling virtual assets; 5. Participation in and provision of financial services related to the offering of an issuer and/or sale of a virtual asset.	

R.22	PC	C.22.2	Under Article 5 of the WID Act and Article 16 of the MOT Act DNFBPs have the same record keeping requirements as FIs. Please see R.11 (Record-keeping) for a full analysis of the existing deficiencies.	(Changed Provision) The provisions for Record keeping (Article 19-21 WMTF) applies to all service providers including DNFBPs. Specifically, Article 19 paragraph 1 states that service providers should retain copies of customer due diligence documents, account information, business correspondence and the results of analyses performed for a period of at least seven years after the termination of the service or after the date of the transaction. In the explanatory notes performed analysis as mentioned in Article 19 paragraph 1 refers to the results of risks assessments of clients. Article 3 paragraph 4 requires that a service provider records the assessment process and the results of identifying and assessing its risks, keep it up to date and provide these results to the supervisory authority upon request.	**This deficiency is addressed.** The record-keeping requirement stated in Articles 19-21 of the recently enacted WMFTF applies to all service providers, including DNFPS. The articles (Art. 19-21) are in accordance with the record-keeping requirements outlined in Recommendation 11. This alignment is achieved by incorporating the following provisions: ▪ ***Article 19 (1)*** *states "service providers shall retain copies of customer due diligence documents, account information, business correspondence and the results of analyzes performed for a period of at least seven years after the termination of the service or after the date of the transaction."* ▪ ***Article 21 (1)*** *notes that "every service provider is obliged to keep the data referred to in Article 20 and all relevant documents concerning national and international transactions in an accessible manner for a period of seven years after the termination of the contract under which the service was provided, the completion of the transaction or seven years after the performance of a service as referred to in Article 1, under d and e. Retained transaction data should enable service providers and competent authorities to adequately reconstruct individual transactions."* ▪ ▪ ***Article 21 (2)*** *notes that "every service provider is obliged, at the request of a competent authority, to store in an accessible manner all data as referred to in Article 20 and all relevant documents concerning national and international transactions, also after the legally required seven years."* Criterion 22.2 is rated as **Met.**

R.22	PC	C.22.3	Under Article 9 sub 1 to 4 of the WID Act, DNFBPs have the same PEPs requirements as FIs. Please see R.12 (PEPs) for a full analysis of deficiencies existing under Article 9 of the WID Act.	(Changed Provision) The deficiency as stated in the MER for Rec 12 has been fully addressed. Reference is made to the comments on Criteria 12.1 -12.4. Reference made to Article 16 of the WMTF	**This deficiency is addressed.** Under the WMTF DNFBPs have the same PEPs requirements as FIs. The deficiencies identified in C12.2, C.12.3 and C.12.4 of the 4th Round MER have now been addressed. These deficiencies had a cascading effect on the criterion. On this basis, the deficiencies identified in C.22.3 have now been addressed. Please see the re-rating of R.12 (PEPs) for a full analysis. Under the Act for the Prevention and Combating of Money Laundering and the Financing of Terrorism (WMFTF), both DNFBPs and FIs are subjected to the same PEPs requirements. The previously identified deficiencies in sections C12.2, C12.3, and C12.4 of the 4th Round Mutual Evaluation Report have been effectively resolved (See re-rating for R.12). These deficiencies had a cascading effect on the evaluation of this criterion. On this basis the deficiencies identified have now been largely addressed. Criterion.22.3 is rated as **Met.**

R.22	PC	C.22.4	Suriname has not identified and assessed the ML/TF risks that may arise in relation to the development of new products and new business practices, neither is there any requirement for DNFBPs to do so. Further, there are no AML/CFT obligations regarding virtual assets (See R.15 for the full details).	(Changed Provision) Article 3 paragraph 3 of the WMTF requires that all service providers take adequate measures to identify and assess the risks of money laundering and the financing of terrorism that may arise from the development and use of new technologies, products and commercial practices, including new service delivery mechanisms. This risk assessment will be performed prior to the introduction or use of such technologies, products and commercial practices. Deficiency for R15 is addressed as follow: In general Article 1 paragraph 1 sub a identifies VASPs as being a service provider. The definition for VASP is set out in Article 1 paragraph 1 sub e as the professional or commercial performance in or from Suriname of one or more of the following activities for or on behalf of a client: 1. exchange between virtual assets and fiat currencies; 2. exchange between one or more others forms of convertible virtual assets; 3. transfer of virtual assets, by carrying out a transaction, where virtual assets moved from one virtual asset address or account to another; 4. custody and/or administration of virtual assets or instruments under control enabling virtual assets; 5. Participation in and provision of financial services related to the offering of an issuer and/or sale of a virtual asset. C15.2(a) in accordance with Article 2 WMTF service providers are obligated to apply a risk-based program that includes the necessary policies, procedures and measures to comply with the rules laid down by or pursuant to this law regarding risk management, internal control measures, customer due diligence, record keeping and unusual transaction reporting.in order to prevent money laundering and terrorism financing. Additionally, Article 3 paragraph 3 states: A service provider takes adequate measures to identify and assess the risks of money laundering and the financing of terrorism that may arise from the development and use of new technologies, products and commercial practices, including new service delivery mechanisms. This risk assessment will be performed prior to the introduction or use of such technologies, products and commercial practices C15.2(b) Article 3 paragraph 4 makes note of the obligation for service providers to record the assessment process and the results of identifying and assessing its risks, keep it up to date and provide these results to the supervisory authority upon request. C15.3c As VASPs are regarded to be a service provider within the WMTF, they are also required to take appropriate steps to identify, assess, manage and mitigate their ML and TF risks (Article 2, 3, 4 of the WMTF)	**This deficiency is addressed.** Under the recently enacted WMTF, DNFBPs are obligated to adhere to new technology requirements outlined in Recommendation 15. ▪ **C15.1 (partly met):** Suriname has not provided indications that the country has identified and assessed the risks of ML/TF that may arise in connection with the development of new products and new business practices. However, under article 3 paragraph 1 of the WMTF, there is a general requirement for a service provider to takes measures to periodically identify and assess its risks of money laundering and terrorism financing, whereby the measures are proportionate to the nature and size of the service provider. ▪ **C1.15.2 (Met):** ▪ ***Sub C.15.2 (a) (met):*** *Article 3 paragraph 3 of the WMTF require a service provider takes adequate measures to identify and assess the risks of money laundering and the financing of terrorism that may arise from the development and use of new technologies, products and commercial practices, including new service delivery mechanisms. The risk assessment must be performed prior to the introduction or use of such technologies, products and commercial practices.* ▪ ***Sub C.15.2 (b) (Met):*** *Under article 3 paragraph 1 of the WMTF, there is a general requirement for a service provider to takes measures to periodically identify and assess its risks of money laundering and terrorism financing, whereby the measures are proportionate to the nature and size of the service provider*. Criterion 22.4 is **Met.**

				C15.4(b) designated supervisor for VASPs in Suriname is the CBvS C15.6(a) minimal supervisory requirements for VASPs are set out in Article 38 and 39 namely Article 38 paragraph 1: The following are charged with supervising compliance with the provisions of or pursuant to Chapters 1 and 2 of this Act: a. the Central Bank of Suriname, as far as the financial and virtual asset service providers are concerned; b. the Supervision and Control Institute for Games of Chance, insofar as it concerns providers of games of chance; c. FIU Suriname, insofar as it concerns the other non-financial service providers Article 38 paragraph 3: The supervisor is authorized to issue guidelines to the service providers under its supervision to promote compliance with this Act. Art 38 par 4: The supervisor may instruct anyone who does not comply with an obligation under Chapters 1 and 2 of this Act and Articles 28 and 29 to comply within a reasonable period set by the supervisor, with regard to points to be indicated in the designation order to follow a certain course of action. A designation may be given to a service provider, and/or its director(s), director(s) and/or other senior management Article 39 paragraph 1: In order to effectuate the supervision as referred to in Article 38, the supervisor is, without prejudice to the powers given by other laws and only insofar as this is reasonably necessary for the performance of their duties, authorized to: a. request all information from the service providers under their supervision; b. obtain access to all data that may be important for the implementation of the aforementioned supervision, such as books, records, documents and other information carriers of the service provider that are in the possession or under the control of any director, director, supervisory director, external auditor or employee personnel of that service provider or under the control of any third party; granting access also includes copying data. Article 39 paragraph 2: The supervisor is authorized to request information and carry out inspections at any service provider under its supervision, as often as it deems necessary. On the basis of its findings and the information obtained during the inspection, the supervisor can oblige the service provider to take such measures as are deemed necessary to promote an adequate regime to combat money laundering and terrorist financing. Article 39 paragraph 3: With a view to exercising supervisory powers, each service provider is obliged to cooperate with the supervisory authority. As such service providers should comply with the requirements as set out in chapters 1, 2, Article 28, 29 and 39 paragraph 1, 2 and paragraph 3 as well as the requirements set out in the guidelines issued by the respective supervisors (Article 38 sub3)	

				C15.6(b) Compelling the production of information is addressed in Article 39 paragraph 1, 2 and 3 (see aforementioned). With regard to imposing a range of disciplinary and financial sanctions by a supervisory authority the Article 38 paragraph 4-10, Article 39 paragraph 4, Article 40 C15.7 No VASPS registered in Suriname. However, under article 1 paragraph 1a, VASP has been classified as a service provider and as such are subject to the Guidelines for reporting Unusual Transactions (October 2019). This guideline provides service providers with guidance on submitting UTRs to the FIU. The FIU also has a standard prescribed feedback form for reporting entities regarding their submissions. C15.8(a and b) comment under c 15.6(b) applies C15.9 preventive measures that mandates VASPs to comply with recommendations 10-21 are regulated within the WMTF. C15.10 In relation to targeted financial sanctions, Article 3 paragraph 4 of the State Decree National Sanctions List mandates that all service providers who are entrusted with frozen funds should report this to the Council on International Sanctions. this requirement is also applicable to VASPS. The definition for service providers within the international sanctions act refers to the definition as stated in the WMTF Article 1 paragraph 1 sub a. C15.11 A supervisor has been designated for VASPS (Article 38 paragraph 1). The legal basis for supervisors for exchanging information with their foreign counterparts are set out in Article 45. Paragraph 2: Anyone who performs or has performed any task pursuant to the application of this Act or decisions taken pursuant to this Act is prohibited from using data or information provided or received pursuant to this Act or from a foreign supervisory authority. have been received, to make further or otherwise use or to disclose them further or otherwise than for the performance of his duties or as required by this law. Paragraph 3: Notwithstanding the provisions of paragraph 2 and without prejudice to the confidentiality obligation imposed by other laws, a supervisor is authorized to provide data or information received under this law or from a foreign supervisory authority to: a. another supervisor or to a foreign supervisory authority; b. other competent authorities within the framework of this Act, insofar as the data or information are useful for the exercise of their statutory duties Paragraph 5: Insofar as the data or information referred to in paragraph 3 has been obtained from a foreign supervisory authority, a supervisor shall not provide it to another supervisor, unless the foreign supervisory authority from which the data or information was obtained has expressly consented to the provision. of the data or information and, where appropriate, has consented to its use for a purpose other than that for which the data or information was provided	

				Par 6: If a foreign supervisory authority requests the supervisory authority that provided the data or information pursuant to paragraphs 3, 4 and 5 to be allowed to use that data or information for a purpose other than that for which it was provided, the supervisory authority will grant that request only in: a. if the intended use does not conflict with paragraphs 3, 4 and 5 or insofar as that supervisory authority has the disposal of that other purpose from Suriname in a manner other than that provided for in this Act, with due observance of the applicable legal procedures for that other purpose obtain data or information; and b. after consultation with the Public Prosecution Service if the request referred to in the preamble relates to an investigation into criminal offences.	

R.22	PC	C.22.5	Pursuant to Article 12 of the WID Act, DNFBPs may rely on the client screening performed by a financial service provider having its registered office in Suriname in regard to a client introduced by a financial service provider. The authorities did not indicate if DNFBPs are allowed to rely on third-party CDD measures conducted by third parties based overseas.	(Changed Provision) In the WMTF the stipulations regarding the use of intermediaries for CDD have been expanded. Service providers may rely on a third party locally or abroad, if they meet the criteria. Article 12 paragraph 1 and 2 states that without prejudice to their own responsibility, service providers can, when conducting customer due diligence as referred to in Article 7 paragraph 2 under a to c and e to g, rely on a customer due diligence conducted by an intermediary or third party, if the following criteria are met: a. the intermediary or third party is also subject to the relevant customer due diligence requirements and has taken measures to comply with these requirements and the record retention requirements; b. the intermediary or third party is supervised by the rules for carrying out customer due diligence in the country of origin of the intermediary or third party; c. the intermediary or third party immediately provides information about the measures taken to conduct customer due diligence and retain data; d. the service provider immediately disposes of the necessary information regarding the identity of the client and ultimate beneficial owner and the details regarding the ownership and control structure of the client, and the purpose and intended nature of the business relationship, and e. is satisfied that the intermediary or third party will promptly make copies of the relevant client information upon request. 2. The ultimate responsibility for the measures referred to in Article 7 paragraph 2 lies with the service provider that calls on the third party.	**This deficiency is addressed.** Article 12, paragraph 1 of the WMTF stipulates that a service provider is permitted to rely on the due diligence conducted by an intermediary or third party on behalf of a customer. The WID Act, which was in force at the time, did not indicate if DNFBPs are allowed to rely on CDD measures conducted by third parties based overseas. Article 1 a – e of the WMTF outlines the criteria that a service provider must fulfil in order to rely on CDD conducted by a third party. These criteria include the following: *a. the intermediary or third party is also subject to the relevant customer due diligence requirements and has taken measures to comply with these requirements and the record retention requirements;* *b. the intermediary or third party is supervised by the rules for carrying out customer due diligence in the country of origin of the intermediary or third party;* *c. the intermediary or third party immediately provides information about the measures taken to conduct customer due diligence and retain data;* *d. the service provider immediately disposes of the necessary information regarding the identity of the client and ultimate beneficial owner and the details regarding the ownership and control structure of the client, and the purpose and intended nature of the business relationship, and* e. *is satisfied that the intermediary or third-party will promptly make copies of the relevant client information upon request.* Criterion 22.5 is rated **Met.**

R.22	**Overall Conclusion**	**R.22 has been upgraded from PC to LC, due to the significant progress made in addressing the deficiencies outlined under c.22.2, c.22.3, c.22.4 and c.22.5 of the 4th Round MER. The amendments made within the WMTF have resolved most of these issues. However, there are still remaining deficiencies related to C22.1 should be addressed.**			
Recommendations where the Standard has changed since the MER					
Other Recommendations rated NC/PC for which the country is not seeking an upgrade					
R.1	PC	C.1.1	The NRA did not cover several relevant areas recommended under the FATF Methodology, these include the NPO sector, legal persons and legal arrangements, and the risk posed by new technologies and VASPs. The NRA's coverage of TF risk was limited.		
R.1	PC	C.1.2	MET		
R.1	PC	C.1.3	MET		
R.1	PC	C.1.4	MET		
R.1	PC	C.1.5	Suriname has not used a risk-based approach to allocate resources and implement measures to prevent or mitigate ML/TF, based on the country's understanding of risk		
R.1	PC	C.1.7(a)	Higher risk scenarios identified via Suriname's NRA were not addressed through changes in the country's AML/CFT regime		
R.1	PC	C.1.7(b)	There are no requirements in place for FIs and DNFBPs to incorporate the findings from the NRA into their risk assessments. The risk mitigation measures are not predicated on the identification of higher risk as evidenced by a national or sectoral risk assessment or other forms of risk assessments.		

R.1	PC	C.1.8	There are no specific legislative provisions in place for Fis and DNFBPs to apply simplified measures to some of the FATF Recommendations. The simplified measures were implemented prior to the completion of the NRA, therefore the measures were not predicated on the country's understanding of its ML/TF risk.		
R.1	PC	C.1.9	The WID Act does not designate a supervisor, therefore this limitation could prevent the supervisors from implementing measures to assess ML and TF risk using a risk-based approach.		
R.1	PC	C.1.10(a)	Suriname's AML/CFT provisions do not require Fis and DNFBPs supervised by the CBvS and the FIUS to document their risk assessments		
R.1	PC	C.1.10(b)& (c)	There are no requirements for Fis to consider all the relevant risk factors in determining the level of overall risk and the relevant mitigation measures.		
R.1	PC	C.1.10(d)	In the case of both Fis and DNFBPs, there is no mechanism in place for reporting entities to provide risk assessment information to their respective competent authorities.		
R.1	PC	C.10.11(a)	There is no requirement for supervised entities to have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified by the country or by the FI or DNFBP		
R.1	PC	C.10.11(b)	There is no requirement for Fis and DNFBPs to monitor the implementation of controls and if required, enhance these measures.		

R.1	PC	C.10.11(c)	There are no requirements for Fis and DNFBPs to take enhanced measures to manage and mitigate higher risks when they are identified.		
R.1	**Overall Conclusion**	**R.1 is rated PC**			
R.2	PC	C.2.1	MET		
R.2	PC	C.2.1	MET		
R.2	PC	C.2.3	MET		
R.2	PC	C.2.4	Suriname has no co-operation and co-ordination mechanisms to combat PF.		
R.2	PC	C.2.5	Suriname has no mechanisms in place for the co-operation and co-ordination between relevant authorities to ensure the compatibility of AML/CFT requirements with Data Protection and Privacy rules and other similar provisions (e.g. data security/localisation)		
R.2	**Overall conclusion**	**R.2 is rated PC**			
R.3	PC	C.3.1	Money laundering having been criminalized under Articles 1 and 3 of the Act on Money Laundering Penalization, doesn't incorporate the purposive element of converting and transferring an item, the acts of being in 'possession' of an item and concealing or disguising 'ownership' of an item.		
R.3	PC	C.3.1	The Act doesn't provide a definition of criminal offence and all of the categories of offences designated by the FATF have not been adopted as terrorist financing does not cover all the elements required under the FATF Standards		

R.3	PC	C.3.4	The definition of "items" in the Act on Money Laundering Penalization does not comply with the FATF standards.		
R.3	PC	C.3.5	MET		
R.3	PC	C.3.8	MET		
R.3	PC	C.3.9	MET		
R.3	PC	C.3.10	The criminal sanctions for legal persons are not proportionate and dissuasive.		
R.3	PC	C.3.11	MET		
R.3	**Overall conclusion**	**R.3 is rated PC**			
R.5	PC	C.5.1	MET		
R.5	PC	C.5.2	Art.72(2) refers to the provision of "opportunity", "means" or "information" and provision or collection of "objects". Objects include all assets, such as movable and immovable property, as well as business and personal rights (art.50a of the Penal Code). However, whilst the authorities have submitted that 'opportunity' and 'means' are meant to cover funds and assets of every kind, there are no clear definitions on the meaning of these terms nor support material to give that interpretation. There is no clear definition of funds in the context of TF offence.		

R.5	PC	C.5.2bis	Financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training is not addressed in Suriname's legislation.		
R.5	PC	C.5.3	MET		
R.5	PC	C.5.4	MET		
R.5	PC	C.5.5	MET		
R.5	PC	C.5.6	MET		
R.5	PC	C.5.7	MET		
R.5	PC	C.5.8	MET		
R.5	PC	C.5.9	MET		
R.5	PC	C.5.10	The financing of terrorist crime (art.71(2) of the Criminal Code) is not specifically addressed. Consequently, TF offences do not apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different 152 country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur since art.4 of the Penal Code provides that the terrorist crimes listed therein are only applicable to crimes committed outside of Suriname and either the act is committed against a Surinamese national or the suspect is in Suriname		

R.5	Overall conclusion	R.5 is rated PC			
R.6	NC	C.6.1(a)	MET		
R.6	NC	C.6.1(b)	There are no mechanisms for identifying targets for designation, based on the designation criteria set out in the relevant United Nations Security Council resolutions		
R.6	NC	C.6.1(c)	An evidentiary standard of proof of "reasonable grounds" or "reasonable basis" is not applied when deciding whether or not to make a proposal for designation		
R.6	NC	C.6.1(d)	The procedures and (in the case of UN Sanctions Regimes) standard forms for listing, as adopted by the relevant committee (the 1267/1989 Committee or 1988 Committee) are not followed		
R.6	NC	C.6.1(e)	As much relevant information as possible on the proposed name, a statement of case which contains as much detail as possible on the basis for the listing, and (in the case of proposing names to the 1267/1989 Committee) whether their status as a designating state may be made known is not provided for.		
R.6	NC	C.6.2(a)	MET		

R.6	NC	C.6.2(b)	In relation to designations pursuant to UNSCR 1373, (i) there are no mechanism(s) for identifying targets for designation, (ii) the appropriate evidentiary standard of proof is not applied, and (iii) there are no procedures for the necessary information to be provided when requesting another country to give effect to actions initiated under the freezing mechanisms.		
R.6	NC	C.6.2(c)	There are no legal authorities and procedures or mechanisms to collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation.		
R.6	NC	C.6.2(d)	According to paragraph C of the Ministerial Decree of Foreign Affairs (2016 no 133), an evidentiary standard of proof of "reasonable grounds" is applied when deciding whether or not to make a proposal for designation. However, such a proposal is conditional upon the opening of a criminal investigation or prosecution by the competent authority for committing, complicity in, or aiding and abetting a terrorist act or an attempt to do so and to prepare or facilitate a terrorist act.		
R.6	NC	C.6.2(e)	There are no procedures to request another country to give effect to the actions initiated under the freezing mechanisms.		
R.6	NC	C.6.3(a)	There are no legal authorities and procedures or mechanisms to collect or solicit information to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation.		

R.6	NC	C.6.3(b)	There are no legal authorities and procedures or mechanisms to operate *ex parte* against a person or entity who has been identified and whose (proposal for) designation is being considered.		
R.6	NC	C.6.4	Targeted financial sanctions are not implemented without delay.		
R.6	NC	C.6.5(a)	The definition of means is contained in Article 1 of the State Decree UN Sanctions Regime (O.G. 2016 no. 34) and it is not as expansive as the FATF definition of "funds or other assets", for example it excludes economic resources and the various forms of property. Additionally, within the State Decree UN Sanctions Regime (O.G. 2016 no. 34) the requirement for all natural and legal persons to freeze, without delay and without prior notice, all balances and other means of those so designated, does not exist. Article 9 of the International Sanctions Act mandates that a party involved in the implementation of this law and thereby obtaining information that they know or may reasonably assume to be of a confidential nature, shall be required to maintain confidentiality of the information. However, this Article doesn't relate to keeping confidential actions that will be taken to apply a freezing measure.		

R.6	NC	C.6.5(b)	The definition of means is contained in Article 1 of the State Decree UN Sanctions Regime (O.G. 2016 no. 34) and it is not as expansive as the FATF definition of "funds or other assets", for example it excludes economic resources and the various forms of property. The finding on the obligation to freeze under (ii), (iii) & (iv) of article 3(2)(a) & (b) of the State Decree National Sanctions List is limited to UNSCR 1373 as it is only capable under the State Decree National Sanctions List and does not apply to UNSCR 1267. There is no definition for 'resources from or produced by funds or other property' which are required to be frozen pursuant to Article 3(2)(b) of the State Decree National Sanctions List, and therefore a conclusive finding cannot be made that it is equivalent to the requirement for the freezing of 'funds or other assets derived or generated from funds or other assets' under this criterion.		
R.6	NC	C.6.5(c)	MET		

R.6	NC	C.6.5(d)	Article 4a of the International Sanctions Act mandates the Minister to communicate decisions on designations to the Council on International Sanctions for the execution of those decisions. Article 5b (2) provides for the Council on International Sanctions to publish within five working days in a digital way the freezing lists and any amendments to these lists for the benefit of service providers. This communication is not done immediately upon taking such a decision. The Council on International Sanctions is also required to make an announcement thereof on its website. There is no requirement for this to be done immediately upon taking such a decision. Article 3(4) of the State Decree National Sanctions List provides that service providers who are entrusted with frozen funds shall forthwith report them to the Council on International Sanctions. Additionally, Article 7 mandates service providers to report to the Unusual Transactions Reporting Center (FIUS) of any request for the provision of a service (attempted transaction) in which a designated person or entity acts as the other party or is involved in any other way. However, such reporting requirements do not extend to transactions or attempted transactions, directed at frozen assets.		
R.6	NC	C.6.6(a)	There is no consideration at the country level to determine whether designated persons no longer meet the criteria for designation, prior to submission to the UN Ombudsman.		

R.6	NC	C.6.6(b)	There are no procedures or mechanisms for delisting pursuant to UNSCR 1373.		
R.6	NC	C.6.6(c)	MET		
R.6	NC	C.6.6(d)	There are no procedures to facilitate review of designations in accordance with any applicable guidelines or procedures, including those of the Focal Point mechanism.		
R.6	NC	C.6.6(e)	MET		
R.6	NC	C.6.6(f)	Procedures for unfreezing funds or other assets of persons or entities inadvertently affected by a freezing mechanism are limited to a service provider recognising the false positive.		
R.6	NC	C.6.6(g)	There is no requirement for communicating de-listing and unfreezing to the financial sector immediately upon taking such action		
R.6	NC	C.6.7	There is no authorisation for the access to funds or other assets, if freezing measures are applied to persons and entities designated by a (supra-) national country pursuant to UNSCR 1373.		
R.7	NC		No steps have been taken to implement this recommendation		
R.7	**Overall conclusion**	**R.7 is….**			
R.8	NC	C.8.1(a)	Suriname has not identified the subset of foundations that fall within the FATF definition of NPOs.		

R.8	NC	C.8.1(b)	Suriname has not conducted any risk assessment to identify the threat posed to the sector by terrorist entities and determine how terrorist actors can abuse NPOs.		
R.8	NC	C.8.1(c)	There is no undertaking by Suriname authorities to review the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for TF support.		
R.8	NC	C.8.1(d)	There has been no periodic reassessment of the NPO sector in Suriname.		
R.8	NC	C.8.2(a)	There are no measures in place that promote accountability, integrity, and public confidence in the administration and management of NPOs.		
R.8	NC	C.8.2(b)	No outreach and educational programmes are being conducted to raise awareness among NPOs and donors about the potential misuse of NPOs by money launders and financiers of terrorism.		
R.8	NC	C.8.2(c)	Suriname has not worked with NPOs to develop and refine best practices to address terrorist financing risk and vulnerabilities, which would also protect NPOs from TF abuse.		
R.8	NC	C.8.2(d)	There are no mechanisms/ process in place that encourages NPOs to only conduct transactions via regulated financial channels.		
R.8	NC	C.8.3	NPOs are not subjected to effective supervision as a designated supervisory authority is not in place.		

R.8	NC	C.8.4	Suriname has not conducted any risk assessment on the NPO sector, and a supervisory body was not appointed to supervise or monitor the NPO sector. Therefore, the country could not demonstrate that effective, proportionate and dissuasive sanctions for violations of established rules, principles, guidelines or frameworks by NPOs or persons acting on behalf of NPOs were in place.		
R.8	NC	C.8.5(a)	There was no evidence or information provided by the jurisdiction of mechanisms for effective co-operation, coordination and information sharing among authorities that hold relevant information on NPOs.		
R.8	NC	C.8.5(b)	The authorities did not demonstrate that they have the investigative expertise and capability to examine NPOs suspected of being exploited by, or actively supporting terrorist activities or terrorist organisations.		
R.8	NC	C.8.5(c)	The authorities did not indicate that investigative bodies' have access to information on the administration and management of particular NPOs during an investigation.		
R.8	NC	C.8.5(d)	There are no mechanisms in place to ensure that when there is suspicion or reasonable grounds to suspect that an NPO is wittingly or unwittingly involved in terrorist financing that this information is promptly shared with competent authorities for them to take preventive or investigative action.		

R.8	NC	C.8.6	There are no appropriate points of contact and procedures to respond to international requests for information regarding NPOs suspected of TF or involvement in other forms of terrorist support		
R.8	**Overall conclusion**	**R.8 is….**			
R.15	NC	C.15.1	Suriname has not identified and assessed the ML/TF risk that may arise in relation to the development of new products and new business practices.		
R.15	NC	C.15.2(a)	In relation to new product assessment, only entities supervised under the BCSS Act are required to submit their product for assessment by the CBvS prior to launch		
R.15	NC	C.15.2(b)	There is no provision for reporting entities to take appropriate measures to manage and mitigate risks relating to new products and practices.		
R.15	NC	C.15.3(a)	Suriname has not identified and assessed the ML and TF risks emerging from virtual asset activities and the activities or operations of VASPs.		
R.15	NC	C.15.3(b)	The country does not have an understanding of the ML/TF risk.		
R.15	NC	C.15.3(c)	VASPs are not required to take appropriate steps to identify, assess, manage and mitigate their ML and TF risks, as required by criteria 1.10 and 1.11.		
R.15	NC	C.15.4(a)	There are no licensing or registration requirements in place for VASPs in Suriname.		

R.15	NC	C.15.4(b)	No competent authority has been identified to provide supervision and monitoring of VASPs.		
R.15	NC	C.15.5	There are no mechanisms in place to identify natural or legal persons that carry out VASP activities in Suriname.		
R.15	NC	C.15.6(a)	There are no supervisory requirements in place for VASPs. Therefore, potential entrants are not subjected to any regulation and risk-based supervision or monitoring by a competent authority		
R.15	NC	C.15.6(b)	There is also no requirement for a supervisory authority to compel the production of information and impose a range of disciplinary and financial sanctions.		
R.15	NC	C.15.7	There is no provision in line with Recommendation 34, requiring competent authorities and supervisors to establish guidelines and provide feedback, which will assist VASPs in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.		
R.15	NC	C.15.8(a)	There are no sanctions, whether criminal, civil or administrative, in place to deal with VASPs that fail to comply with AML/CFT requirements.		
R.15	NC	C.15.8(b)	There are no sanctions, whether criminal, civil or administrative, in place to deal with VASPs that fail to comply with AML/CFT requirements.		
R.15	NC	C.15.9(a) and (b)	There are no preventive measures in place that mandates VASPs to comply with recommendations 10 to 21. There is		

			no threshold value defined for virtual asset transactions.		
R.15	NC	C.15.10	In relation to targeted financial sanctions, article 3 paragraph 4 of the State Decree National Sanctions List mandates that all service providers (FIs and DNFBPs) who are entrusted with frozen funds should report this to the Council on International Sanctions. The authorities however did not demonstrate that these requirements are also applicable to VASPs.		
R.15	NC	C.15.11	There is no legal basis for international co-operation in relation to VASP on ML, TF and predicate offences as set out in Recommendation 37 - 40.		
R.15	NC	C.15.11	Suriname has not restricted VASP from operating in the country, however, the country is yet to identify a supervisor for these providers.		
R.15	NC	C.15.11	There is no legal basis for permitting relevant competent authorities (e.g. law enforcement agencies) to exchange information on issues related to VAs and VASPs with non-counterparts in the absence of a supervisory framework.		
R.15	**Overall conclusion**	**R.15 is rated NC**			
R.19	PC	C.19.1	MET		
R.19	PC	C.19.2	Suriname has not defined the specific countermeasures that are to be applied proportionate to the risks: (a) when called upon to do so by the FATF; and (b) independently of any call by the FATF to do so.		

R.19	PC	C.19.3	Suriname's legislation has no specific measures in place to ensure that FIs are advised of concerns about weaknesses in the AML/CFT systems of other countries.		
R.19	**Overall conclusion**	**R.19 is rated PC**			
R.24	NC	C.24.1	There are no processes in place for obtaining and recording beneficial ownership information with respect to each type of legal person.		
R.24.2	NC	C.24.2	Suriname has not assessed the ML/TF risks associated with all types of legal persons created in the country.		
R.24	NC	C.24.3	There is no requirement for any of the legal persons to register the address of their registered office and basic regulatory powers.		
R.24	NC	C.24.4	There is no requirement for any of the legal persons to maintain the information set out in criterion 24.3.		
R.24	NC	C.24.5	Although Limited Liability Companies (by shares) maintains a register, it does not contain all of the shareholder information. There is no requirement that this information should be maintained within Surname at a location notified to the trade registry.		
R.24	NC	C.24.6	There are no mechanisms to ensure that information on the beneficial ownership of a legal person is obtained by that legal person and available at a specified location; or can be otherwise determined		

			in a timely manner by a competent authority.		
R.24	NC	C.24.7	There are no measures to ensure that beneficial ownership information is accurate and as up-to-date as possible.		
R.24	NC	C.24.8	There are no measures to ensure that companies co-operate with competent authorities to the fullest extent possible in determining the beneficial owner.		
R.24	NC	C.24.9	No requirement for beneficial ownership information and associated records to be held by or on behalf of the legal person in the circumstances described under c.29.9.		
R.24	NC	C.24.10	Competent authorities, and in particular law enforcement authorities, do not have all the powers necessary to obtain timely access to basic and beneficial ownership information held by relevant parties.		
R.24	NC	C.24.11	MET		
R.24	NC	C.24.12	There are no mechanisms to prevent nominee shares and nominee directors from being misused.		
R.24	NC	C.24.13	The sanctions for a natural and legal person failing to comply with the requirements are not proportionate and dissuasive.		
R.24	NC	C.24.14	There is no provision within the Trade Register Act which facilitates access by foreign competent authorities to the basic information held.		

R.24	NC	C.24.15	There is no monitoring of the quality of assistance received from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.		
R.24	**Overall conclusion**	**R.24 is rated NC**			
R.25	NC	C.25.1(a)	MET		
R.25	NC	C.25.1(b)	The financial and non-financial service providers are not required to hold basic information on other regulated agents and service providers, including investment advisors or managers, accountants and tax advisors.		
R.25	NC	C.25.1(c)	The deficiency in criterion 25.1(b) has a cascading effect here.		
R.25	NC	C.25.2	No measures are in place which provide for a timeframe for updating client information. The deficiency in criterion 25.1(b) has a cascading effect here.		
R.25	NC	C.25.3	There are no measures which impose an obligation on service providers to disclose their status to financial institutions and DNFBPs when forming a business relationship or carrying out an occasional transaction above the threshold.		
R.25	NC	C.25.4	MET		
R.25	NC	C.25.5	There are no provisions for other competent authorities, and in particular		

			LEAs, to have all the powers necessary to obtain timely access to information held by trustees or by FIs and DNFBPs regarding the beneficial ownership and control of the foreign trust.		
R.25	NC	C.25.6	There are no measures which provide for international co-operation in relation to information, including beneficial ownership information, on trusts and other legal arrangements, on the basis of Recommendations 37 and 40.		
R.25	NC	C.25.7	The deficiency in criterion 25.1(b) has a cascading effect here.		
R.25	NC	C.25.8	There are no proportionate and dissuasive sanctions, whether criminal, civil or administrative, for failing to grant to competent authorities timely access to information referred to in c.25.1.		
R.25	**Overall conclusion**	**R.25 is rated NC.**			
R.26	PC	C.26.1	Whilst article 22 of the MOT Act designates the CBvS as the AML/CFT supervisor for FIs, CBvS is only entrusted with supervising compliance with the provisions of or pursuant to the MOT Act which only includes disclosure of unusual transactions. Therefore, there is no provision that designates CBvS as being responsible for the supervision and monitoring of FIs with AML/CFT requirements.		

R.26	PC	C.26.1	Whilst FIs have AML/CFT requirements under the WID Act, the legislation does not designate an AML/CFT supervisor.		
R.26	PC	C.26.2	There is no prohibition on the establishment or continued operation of shell banks		
R.26	PC	C.26.3	Whilst the BCSS Act, MTOS Act, CM Act and the Insurer's Directive, March 10,2021, refers to fitness and proprietary procedures conducted for holders of a "qualified holding", 185 there are no specific measures for beneficial owners as defined by the FATF. Therefore, the fitness and proprietary measures for beneficial owners are not adequately defined.		
R.26	PC	C.26.4(a)	The Group II Regulations (6-10) make no reference to AML/CFT requirements.		
R.26	PC	C.26.4(a)	Suriname has not defined the nature and extent of application of consolidated AML/CFT group supervision policies and procedures.		
R.26	PC	C.26.4(a)	Also, there are no guidelines in line with IOSCO and the AML/CFT guideline for insurance companies, which is anticipated to be based on the IAIS principles, is still in draft.		
R.26	PC	C.26.5	The frequency and intensity of AML/CFT supervision (on-site and off-site) is not adequately based on the ML/TF risks present in the country and ML/TF characteristics and risks for the FIs that are part of a group.		

R.26	PC	C.26.5	The frequency and the triggers for the periodic review of the financial entities risk assessments are not documented, to ensure that the risk assessments for the FIs are kept up to date.		
R.26	PC	C.26.5	The risk-based supervision framework (for both the off-site monitoring and on-site inspections) for the credit unions, banks, insurance and securities is still under development.		
R.26	PC	C.26.5	Suriname Authorities have not demonstrated the determinants for the frequency and intensity of on-site and off-site AML/CFT supervision for securities and insurance companies.		
R.26	PC	C.26.5	The monitoring by conducting risk-focused AML/CFT on-site inspections is not specifically mentioned in the policies but is now mentioned in the draft Manual AML/CFT On-site for insurance and securities sectors.		
R.26	**Overall conclusion**	**R.26 is rated PC**			
R.27	PC	C.27.1	The CBvS is identified as the AML supervisory authority for financial service providers under the MOT Act. This authority only extends to supervision of unusual transactions reporting. As it relates to supervision and monitoring in relation to compliance with the WID Act (Identification Requirements for Service Providers Act), the Act does not grant the CBvS supervisory powers.		

R.27	PC	C.27.2	The remit of the MOT Act only extends to the supervision of FIs in relation to compliance concerning the disclosure of unusual transactions. Suriname's other principal AML/CFT legislation, the WID Act, which deals with identification requirements does not identify an AML/CFT supervisor.		
R.27	PC	C.27.3	The CBvS' authority to compel the production of information deemed relevant to the monitoring of compliance is limited to prudential supervision.		
R.27	PC	C.27.3	The provisions of the MOT Act regarding the production of information only relates to the FIUS requesting information to the reporting of unusual transactions (Art. 22a).		
R.27	PC	C.27.3	As it relates to insurance companies and pension funds, the supervisor is not empowered by legislation (Bank Act and MOT Act) to compel the production of any information relevant to monitoring compliance with the AML/CFT requirements.		
R.27	PC	C.27.4	As it relates to the WID Act, the CBvS may have difficulty enforcing the sanctions outlined therein given that it is not explicitly empowered to supervise compliance under the act.		
R.27	PC	C.27.4	The CBvS' power to impose a fine for non-compliance with the BCSS Act (Article 56) is in relation to prudential supervision.		

R.27	PC	C.27.4	The CBvS' power to impose a fine or revoke the licence of a money service provider for non-compliance with the conditions of the licence is in relation to prudential supervision.		
R.27	PC	C.27.4	In relation to sanctions, the current legislation relating to pension funds and insurance companies does not contain disciplinary sanctions for non-compliance and does not contain the power to withdraw, restrict or suspend these entity licences in relation to AML/CFT matters.		
R.27	PC	C.27.4	As it relates to stock brokerage firms or the stock exchange, the sanctions outlined in Articles 34 and 35 of the Capital Market Act are not in relation to licensees' failure to comply with AML/CFT requirements.		
R.27	**Overall conclusion**	**R.27 is rated PC**			
R.28	PC	C.28.1(a)	MET		
R.28	PC	C.28.1(b)	There are no legal or regulatory measures to prevent criminals or their associates from holding significant or controlling interest, or holding a management function, or being an operator of a casino.		
R.28	PC	C.28.1(c)	The GSCI's supervisory responsibility under the MOT Act is limited to the disclosure of unusual transactions, consequently, it has no authority to supervise casinos of compliance with other AML/CFT obligations (under the WID Act).		

R.28	PC	C.28.4(a)	As it relates to the WID Act which details identification requirements for service providers, there are no provisions in place that grants the supervisors the power to supervise, monitor and impose sanctions on DNFBPs pursuant to the WID Act.		
R.28	PC	C.28.4(a)	There are no provisions under the WID Act in place that grants the FIUS supervisory powers pursuant to this Act.		
R.28	PC	C.28.4(b)	There are no measures are in place to prevent criminals or their associates from being professionally accredited or holding (or being the beneficial owner of) a significant or controlling interest or holding a management function in a DNFBP.		
R.28	PC	C.28.4(c)	Whilst the FIUS is empowered to impose financial and administrative sanctions on DNFBPs that fail to comply with reporting requirements (Article 22 of the MOT Act), there are no provisions regarding the authority to enforce accordingly.		
R.28	PC	C.28.5(a)	In relation to the Council on International Sanctions, the Council is yet to develop a supervisory framework to monitor compliance with the Act.		
R.28	PC	C.28.5(a)	The authorities did not indicate the mechanisms in place to determine the frequency and intensity of AML/CFT supervision of DNFBPs.		
R.28	PC	C.28.5(b)	For both casinos and other DNFBPs, supervision is not conducted on a risk-sensitive basis.		

R.28	Overall conclusion	R.28 is rated PC			
R.29	PC	C.29.1	MET		
R.29	PC	C.29.2	MET		
R.29	PC	C.29.3(a)	Additional information can only be requested from the reporting entity which filed the UTR.		
R.29	PC	C.29.(b)	The institutional and administrative framework required for the FIUS to access government held data and information has not been put in place, therefore the FIUS only has access to some government institutions, the KPS, financial institutions, the CCI and Industry and open sources.		
R.29	PC	C.29.4	MET		
R.29	PC	C.29.5	No provisions for the use of dedicated, secure and protected channels for disseminating information.		
R.29	PC	C.29.5	The FIUS however does not have the power to disseminate the results of its analysis directly and can only do so through the PG.		
R.29	PC	C.29.5	Dissemination to other competent authorities, other than those entrusted with the investigation and prosecution of criminal offences (KPS and OvJ) can only be done once the precondition of an existing MOU is met.		

R.29	PC	C.29.6(a)	No actual rules to govern how information is handled, securely stored, and disseminated.		
R.29	PC	C.29.6(b)	The Code of Conduct is limited as it does not address factors such as security clearance levels and the handling and dissemination of sensitive information.		
R.29	PC	C.29.6(c)	MET		
R.29	PC	C.29.7(a)	The FIUS however does not have the power to disseminate the results of its analysis directly and can only do so through the PG.		
R.29	PC	C.29.(b)	No provisions for the FIUS to independently engage with its domestic counterparts.		
R.29	PC	C.29.7(c)	MET		
R.29	PC	C.29.7(d)	The FIUS is not able to deploy the human and budgetary resources necessary to carry out its functions; budgetary allocations are unknown; the process for recruiting and retaining staff and the duties and functions of the Director are not prescribed; the PG is entrusted with supervising the FIUS even though Article 2 of the MOT established the unit as an independent body.		
R.29	**Overall conclusion**	**R.29 is rated PC**			
R.30	PC	C.30.1	The JIT has been designated with responsibility for investigating the cross-border element of TF. However, there no law enforcement agency specifically		

			designated with responsibility for ensuring that all elements of TF are properly investigated.		
R.30	PC	C.30.2	MET		
R.30	PC	C.30.3	MET		
R.30	PC	C.30.4	NA		
R.30	PC	C.30.5	NA		
R.30	**Overall conclusion**	**R.30 is rated PC.**			
R.31	PC	C.31.1	MET		
R.31	PC	C.31.2(a)	There are no measures in place in respect to undercover operations.		
R.31	PC	C.31.2(b)	Competent authorities conducting investigations cannot utilise wiretapping because the Authorities and telecommunication service providers have not been able to agree on how to meet the costs associated with obtaining the additional equipment and personnel required carry out the wiretapping.		
R.31	PC	C.31.2(c)	There are no measures in place in respect to accessing computer systems.		
R.31	PC	C.31.2(d)	There are no measures in place in respect to controlled delivery.		
R.31	PC	C.31.3(a)	There are no measures to support the identification, in a timely manner, whether natural or legal persons hold or control accounts.		

R.31	PC	C.31.(b)	There are no measures to support competent authorities having a processto identify assets without prior notification to the owner.		
R.31	PC	C.31.4	There are no measures to support competent authorities being able to ask for all relevant information held by the FIUS, when conducting investigations of ML, associated predicate offences and TF.		
R.31	**Overall conclusion**	**R.31 is rated PC**			
R.32	PC	C.32.1	There is no information on whether declarations are also required for the physical cross-border transportation through mail or cargo.		
R.32	PC	C.32.2	MET		
R.32	PC	C.32.3	NA		
R.32	PC	C.32.4	There are no measures which grants competent authorities the authority to request and obtain further information from the carrier with regard to the origin of the currency or BNIs, and their intended use, upon discovery of a false declaration of currency of BNI or a failure to disclose them.		
R.32	PC	C.32.5	MET		
R.32	PC	C.32.6	MET		
R.32	PC	C.32.7	MET		

R.32	PC	C.32.8	There are no provisions for specifically stopping or restraining currency or BNIs for a reasonable time in order to ascertain whether there may be evidence of ML/TF in cases where there is suspicion of ML/TF or predicate offences or where there is a false declaration.		
R.32	PC	C.32.9	No measures which specifically address the requirement that records should be retained when: a declaration or disclosure exceeds the prescribed threshold; or when there is a false declaration; or when there is suspicion of ML/TF.		
R.32	PC	C.32.10	MET		
R.32	PC	C.32.11	MET		
R.32	**Overall conclusion**	**R.32 is rated PC**			
R.35	PC	C.35.1	Regarding R8, the NPO sector is not regulated, therefore there are no sanctions in place to deter ML/TF.		
R.35	PC	C.35.1	Sanction applicable under the MOT act are in relation to supervision regarding unusual transactions.		
R.35	PC	C.35.1	In relation to the WID Act, the supervisor may find it difficult to impose sanctions outlined in the Act as it does not identify the relevant AML/CFT supervisors. Further, the sanctions outlined in the BCSS Act are mainly in relation to prudential supervision.		
R.35	PC	C.35.1	As it relates to VA/VASP, Suriname does not have a supervisory framework for		

			VA/VASP, as a result, there are no sanctions in place to dissuade ML/TF.		
R.35	PC	C.35.2	The Directors and senior management of service providers are not captured for AML/CFT breaches.		
R.35	**Overall conclusion**	**R.35 is rated PC**			
R.36	PC	C.36.1	MET		
R.36	PC	C.36.2	The Vienna Convention is not fully implemented as there are no measures in relation to Article 5(5) on sharing of proceeds or property confiscated; Article 6 on extradition in the absence of a treaty; Article 11 on controlled delivery; Article 15 on commercial carriers; and Article 17 on illicit traffic by sea and Article 19 on the use of mails.		
R.36	PC	C.36.2	The Palermo Convention has not been fully implemented as there are no measures in relation to Article 14(3) on sharing of proceeds or property confiscated, Article 16 on extradition in the absence of a treaty, Article 20 on special investigative techniques and Article 26 on measures to enhance co-operation with law enforcement authorities.		
R.36	PC	C.36.2	The Merida Convention is not fully implemented as there are no measures in relation to Article 44 on extradition in the absence of a treaty and Article 50 on special investigative techniques.		
R.36	PC	C.36.2	The Terrorist Financing Convention has been adopted, but the offence at Article 2		

			has not been implemented within Surinamese law		
R.36	**Overall conclusion**	**R.36 is rated PC**			
R.37	PC	C.37.2	There are no clear processes for the timely prioritisation and execution of mutual legal assistance requests.		
R.37	PC	C.37.2	No formal provisions for the maintenance of a case management system to monitor the progress on requests.		
R.37	PC	C.37.2	No written procedures on how requests are to be managed at the DIRSIB.		
R.37	PC	C.37.3	It is unreasonable and unduly restrictive that a request for assistance would be refused if made for the purpose of an investigation into offences for which a person was prosecuted, the prosecution was discontinued, or the suspect is prosecuted in Suriname		
R.37	PC	C.37.4	Mutual legal assistance requests can only be granted based on a treaty and the authorisation of the Surinamese government.		
R.37	PC	C.37.5	The Criminal Procedure Code doesn't provide for the confidentiality of information contained within the mutual legal assistance requests received by Suriname.		
R.37	PC	C.37.6	MET		
R.37	PC	C.37.7	NA		

R.37	PC	C.37.8	The deficiencies identified in criterions 31.2 and 36.2 having a cascading effect on this criterion.		
R.37	**Overall conclusion**	**R.37 is rated PC.**			
R.38	NC	C.38.1	The limitations which have a cascading effect on this Recommendation are that (i) the definition of objects at Article 50a(5) of the Criminal Code is not as expansive as the FATF definition of property, (ii) all of the FATF designated categories of offences have not been adopted as the criminalisation of terrorist financing does not cover all the elements required under the FATF Standards.		
R.38	NC	C.38.2	According to Article 11(2)(a) of the Law Take-Over and Transference Execution Criminal Judgements, at the request of a foreign state, objects can only be confiscated if according to Surinamese law it is permitted.		
R.38	NC	C.38.2	According to Articles 9, 50, 50a, 54b & 54c of the Criminal Code, the confiscation of objects can only occur upon the conviction of a person for a criminal offence.		
R.38	NC	C.38.2	Suriname doesn't have the authority to provide assistance to requests for co-operation made based on non-conviction-based confiscation proceedings and related provisional measures, even at a minimum in circumstances when a perpetrator is unavailable by reason of death, flight, absence, or the perpetrator is unknown.		

R.38	NC	C.38.3	The limitations identified at c.38.1 have cascaded unto this criterion.		
R.38	NC	C.38.4	There are no mechanisms or laws in Suriname which enables them to share confiscated property with other countries, in particular when confiscation is directly or indirectly a result of co-ordinated law enforcement actions.		
R.38	**Overall conclusion**	**R.38 is rated PC.**			
R.39	PC	C.39.1(a)	MET		
R.39	PC	C.39.1(b)	No information on processes for prioritisation and existence of a case management system for timely execution of requests were provided.		
R.39	PC	C.39.1(c)	MET		
R.39	PC	C.39.2(a) &(b)	The Decree on extradition states that (a) Extradition will take place only pursuant to a Treaty and Surinamese are not to be extradited. However, while article 466a of the Criminal Proceeding Code authorises the AG to make requests to foreign jurisdictions for legal assistance, this provision is insufficient to comply with the requirements of c39.2(b) as it places no obligation on Suriname, at the request of the country seeking extradition, to pursue a domestic prosecution for the offences set forth in the request		
R.39	PC	C.39.3	MET		
R.39	PC	C.39.4	MET		

R.39	**Overall conclusion**	**R.39 is rated PC**			
R.40	PC	C.40.1	The exchange of data or information by the CBvS cannot be done spontaneously and is only possible if there exists a concluded information exchange agreement with the relevant authority or body.		
R.40	PC	C.40.1	In the event that the data or information involves an investigation into criminal offences, it can only be supplied with the prior permission from the Attorney General or the Court of Justice.		
R.40	PC	C.40.1	The MOT Act also allows the FIUS to exchange data from the FIUS register with agencies outside of Suriname whose duties are comparable to those of the FIUS. This can only take place on the basis of a treaty/convention or a memorandum of understanding. The exchange of this data cannot be done spontaneously. Whilst the AG can provide international legal assistance this assistance is not possible spontaneously.		
R.40	PC	C.40.1	No information was available on whether the other competent authorities (AG; KPS; GSCI; Council on International Sanctions) in Suriname can provide international co-operation in relation to ML and associated predicate offences.		
R.40	PC	C.40.2(a)	There are legal bases for providing for co-operation on the part of the judiciary, KPS, CBvS and the FIUS. However, no information was available on the other		

			competent authorities (AG; GSCI; Council on International Sanctions).		
R.40	PC	C.40.2(b)	The Assessment Team has not been provided with information on the competent authorities' satisfaction of sub-criteria (b).		
R.40	PC	C.40.2(c)	The Assessment Team has not been provided with information on the competent authorities' satisfaction of sub-criteria (c).		
R.40	PC	C.40.2(d)	The Assessment Team has not been provided with information on the competent authorities' satisfaction of sub-criteria (d).		
R.40	PC	C.40.2(e)	The Assessment Team has not been provided with information on the competent authorities' satisfaction of sub-criteria (e).		
R.40	PC	C.40.3	Whilst the CBvS and the FIUS has signed MOUs, it is not known whether these were done in a timely manner and whether the other competent authorities (AG; KPS; GSCI; Council on International Sanctions) are able to execute MOUs in a timely manner.		
R.40	PC	C.40.4	No legislative or other avenue for requesting competent authorities to provide feedback in a timely manner on the use and usefulness of the information obtained.		
R.40	PC	C.40.5(a)	Requests on fiscal matters can only be granted if there is an existing treaty and		

			the authorization of the Surinamese government must be obtained.		
R.40	PC	C.40.5(b)	MET		
R.40	PC	C.40.5(c)	MET		
R.40	PC	C.40.5(d)	MET		
R.40	PC	C.40.6	Other than the CBvS, no authoritative information was provided on safeguards available to the other (AG; FIUS; KPS; GSCI; Council on International Sanctions) competent authorities for ensuring that information exchanged is used for the purpose intended.		
R.40	PC	C.40.7	For the CBvS, the MTOS Act provides no requirement no requirement that their duty of confidentiality be consistent with their respective obligations concerning privacy and data protection and no authoritative information was provided on the AG; FIUS; KPS; GSCI; Council on International Sanctions.		
R.40	PC	C.40.8	Competent authorities are able to conduct inquiries on behalf of foreign counterparts. The exchange of information is limited to the terms of the mutual legal assistance treaty concluded with the foreign counterpart and doesn't extend to all information that would be obtainable by them if such inquiries were being carried out domestically.		
R.40	PC	C.40.9	This exchange will only take place on the basis of a treaty/convention or a		

			Memorandum of Understanding (Article 9.2).		
R.40	PC	C.40.10	The FIUS has not shown that it provides feedback to its foreign counterparts, upon request and whenever possible, on the use of the information provided as well as on the outcome of the analysis conducted, based on the information provided.		
R.40	PC	C.40.11(a)	MET		
R.40	PC	C.40.11(b)	The FIUS is not able to exchange information subject to the principle of reciprocity but rather subject to a treaty, convention or MOU.		
R.40	PC	C.40.12	Whilst article 46 of the BCSS Act allows CBvS to exchange information with foreign supervisors, the CBvS is only entrusted with supervising compliance with the provisions of or pursuant to the MOT Act which only includes disclosure of unusual transactions therefore the information permitted to be exchanged is limited.		
R.40	PC	C.40.13	Article 46 section 1(e) of the BCSS Act creates an inhibition on the part of the CBvS' access to complete information to perform its AML/CFT functions for the credit institutions.		
R.40	PC	C.40.14(a)	Suriname did not demonstrate that provisions are in place for the exchange of regulatory information (on the domestic system, and general information on the financial sector) outside of information available on the CBvS' website		

R.40	PC	C.40.14(b)	Outside of the medium created by the Caribbean Group of Banking Supervisors, the authorities did not demonstrate that other mechanisms are in place that would allow for the sharing of prudential information among supervisors.		
R.40	PC	C.40.14(c)	Sharing of AML/CFT information by the CBvS is restricted to financial institutions offering credit.		
R.40	PC	C.40.15	No information was provided regarding the legal basis upon which the CBvS can conduct inquiries on behalf of foreign counterparts and the inquiries are only in relation to prudential information and access is limited to credit institutions and not the full range of FIs as defined in the FATF Recommendations.		
R.40	PC	C.40.16	Whilst article 46 (1)(c) of the BCSS Act requires that the CBvS ensures that its prior consent is obtained from the requested supervisor. The provisions laid out in the BCSS Act are applicable to credit entities and there are no laws with similar provisions for other FIs.		
R.40	PC	C.40.17	Outside of INTERPOL, no information was available regarding sharing domestically available information through other organisations, like ARIN CARIB.		
R.40	PC	C.40.18	MET		
R.40	PC	C.40.19	No information was available on the ability of the KPS and the AG to form joint investigative teams to conduct co-		

			operative investigations and establish bilateral and multilateral arrangements.		
R.40	PC	C.40.20	The authorities did not demonstrate that Suriname has permitted its competent authorities to exchange information indirectly with non-counterparts and that measures are in place that ensures that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made.		
R.40	**Overall conclusion**	**R.40 is rated PC.**			