Appendix I: List of compulsory requirements as set out in the Provisions and Guidelines on the Detection and Deterrence of Money Laundering and Terrorist Financing.

Credit institutions

1.	II.2. Policy statement	Each credit institution's Board of Supervisory Directors and senior management must issue a policy statement that clearly expresses the credit institution's commitment to combat the abuse of its facilities, financial products, and services for the purpose of money laundering and terrorist financing. The policy statement must state the institution's intention to comply with current anti-money laundering and terrorist financing legislation as well as provisions and guidelines, in particular the laws and guidelines regarding the identification of clients and the reporting of unusual transactions. The policy statement must cover also the following items. • The implementation of a formal system of internal control to identify (prospective) clients and deter, detect, and report unusual transactions, and keep adequate records of clients and transactions; • The appointment of one or more compliance officer(s) at management level responsible for ensuring day-to-day compliance with these procedures. The officer(s) must have the authority to investigate unusual transactions extensively; • A system of independent testing of the policies and procedures by the credit institution's internal audit personnel, compliance department, or by a competent external source to ensure their effectiveness; • The preparation of an appropriate training plan for and training of personnel to increase employees' awareness and knowledge in the area of money laundering and terrorist financing prevention and detection.

2.	II.2.A. Detection and deterrence of money laundering	Credit institutions have the obligation to identify their (prospective) personal or corporate clients/customers before rendering them financial services. Management must maintain an information program to inform those clients of the objectives of the relevant ant-money laundering legislation and inherent requirements for credit institutions. Internal procedures must clearly indicate for which financial services clients or their representatives must be identified and which identification documents are acceptable. The required information must be regularly updated and adequately documented. Credit institutions must have and follow clear standards on what records must be kept on the aforementioned areas, including individual transactions, account files, and business correspondence, and on their retention period for current as well as terminated accounts or business relationships. An important objective for credit institutions is to be able to retrieve this information, without any undue delay.
3.	II.2.A. Identification checklist	The Central Bank requires the credit institution to implement a checklist containing identification and/or transaction information and to maintain a centralized record keeping system to retain copies.
4.	II.2.A Foreign branches and subsidiaries	Credit institutions are required to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local (i.e., host country) laws and regulations permit. Credit institutions must be required to pay particular attention that this principle is observed with respect to their branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations. Where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (i.e., host country) laws and regulations permit. Credit institutions are required to inform the Central Bank when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (i.e., host country) laws, regulations, or other

		measures.
5.	II.2.A. Customer Due Diligence	Credit institutions must develop clear customer acceptance policies and procedures, including a description of the categories of customer likely to pose a higher than average risk to the credit institution. The policy must ensure that transactions will not be conducted nor accounts opened with (prospective) customers who fail to provide satisfactory evidence of their identity.
6.	II.2.A. Source of funds declaration form	The source of funds declaration form must be used in the opening of accounts and/or the transferring of funds, and when accepting funds from occasional customers and non correspondent banks. Where it is reasonable to believe that a requested transaction is connected with criminal activity or if the client refuses to sign a "source of funds declaration", and there is no credible explanation to dispel concerns, the credit institution must refuse to execute the requested transaction to ensure that the minimum standards are met, but still report it to the Unusual Transactions Reporting Center (FIU/MOT).
7.	II.2.A. Ongoing Due Diligence	The efforts to "know your customer" must continue even after the client has been identified. Ongoing due diligence must include also the scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds. If doubts arise relating to the identity of the client after the client has been accepted and accounts have been opened, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the Financial Intelligence Unit (FIU). The Dutch translation for the Financial Intelligence Unit is Meldpunt Ongebruikelijke Transacties (MOT).
8.	II.2.A. Updated copies of identification document	If the institution becomes aware, that it lacks sufficient information about an existing customer, the institution must retain updated copies of the identification document. Credit institutions are required to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

		For identification purposes, the credit institution must distinguish the following customers and their transactions: (a) transactions (including the opening of an account) with (prospective) account holders based on a permanent relationship; (b) transactions with non-account holders or occasional customers; and (c) non-account holders' requests for provision of safekeeping custody services.
9.	II.2.A. Verification identity of resident customers	The identity of a resident individual customer must be verified when a business relationship is established with the customer. The identity of the customer also must be verified when the credit institution has doubts about the veracity or adequacy of the identification data obtained from existing customers.
10.	II.2.A. Identification Non-resident customers	For nonresident clients a copy of the identification document is sufficient, under the condition that the relevant document is accompanied by a certified extract of the civil registry of births, marriages and deaths of the place of residence of the party or that the document is certified by a notary public, embassy or consulate. The name, address and telephone number of the notary public, embassy or consulate including the name and contact details of the officer who signed for certification must be clearly indicated. The submitted copy of the identification document, including the photograph, must be clearly legible.
11.	II.2.A.Policies and procedures Non-face-to-face customers	Credit institutions are required to have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions. These policies and procedures must apply when establishing customer relationships and when conducting ongoing due diligence. Measures for managing the risks must include specific and effective CDD procedures that apply to non-face-to-face customers.
12.	II.2.A. Verification of the identity of non-resident customers	Verification of the identity of nonresident clients must be obtained by reference to one or more of the following, as deemed practical and appropriate: • existing banking relationships of the prospective

		customer; • international or home country telephone directory; • personal reference by a known account holder; • embassy or consulate in home country of address provided by the prospective client; • comparison of signature if a personal account cheque is tendered to open the account; and • if provided, cross reference of address printed on personal cheque to permanent address provided by client on standard application form. Credit institutions must pay special attention to nonresident customers and understand the reasons why the customer has chosen to open an account in Curaçao or Sint Maarten.
13.	II.2.A. Identification of PEP's	Credit institutions must conduct enhanced due diligence for politically exposed persons (PEPs), their families and associates. The institution's decision to enter into business relationships with PEPs must be taken at its senior management level. The institution must make reasonable efforts to ascertain that the PEP's source of wealth and source of funds/ income is not from illegal activities and where appropriate, review the customer's credit and character and the type of transactions the customer would typically conduct. Credit institutions must not accept or maintain a business relationship if the institution knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, financial institutions must obtain senior management approval to continue the business relationship. Where the financial institution is in a business relationship with a PEP, they must conduct enhanced ongoing monitoring on that relationship.
14.	II.2.A. Identification of corporate customers	It is important to identify the nature of the business, account signatures, and the (ultimate) beneficial owner(s) of corporate customers. Credit institutions also must obtain personal information on the managing and/or supervisory directors. Copies of the identification documents of all account signatories, including the directors without signing authority on the corporate client's accounts, must be kept on file. The procedures for the identification of personal customers must be applied for the mentioned account signatures' director(s) and all (ultimate)

		beneficial owners (UBO) holding a qualifying interest in the company. Credit institutions must ascertain the identity of corporate customers based on reliable identification documents, with preference for originals and official documents attesting to the legal existence, and structure of a company or legal entity. The identity, existence and nature of the corporate customer must be established with the aid of a certified extract from the register of the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation. The extract or the identification document must contain at least the information stipulated by the Minister of Finance.
15.	II.2.A. Identification in case of representation	If the customer acts for a third party or that third party also acts for another third party, the credit institution must be bound to also establish the identity of each third party.
16.	II.2.A. Identification of clients with nominee accounts	All credit institutions that provide nominee services must know the true identity of the person/persons (resident or nonresident) for whom assets are held or are to be held, including the ultimate beneficial owner(s). The identity of these clients must be established in accordance with the identification procedures.
17.	II.2.A. Beneficial owner declaration	A credit institution must have each corporate account holder complete and sign for each account a beneficial owner declaration form for all accounts.
18.	II.2.A. Anonymous accounts	Anonymous accounts or accounts in fictitious names are prohibited.
19.	II.2.A. Numbered accounts	Credit institutions are required to maintain numbered accounts in such a way that full compliance can be achieved with the FATF Recommendations.
20.	II.2.A. Reliance on intermediaries or other third parties	These steps must be taken by credit institutions when relying on intermediaries or other third parties to perform aforementioned elements of the CDD process: • immediately obtain from the third party the necessary information concerning the elements of the CDD process; • satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay, however, not longer

		than within a timeframe of 2 working days; • satisfy themselves that the third party is AML/CFT adequately regulated and supervised, and has measures in place to comply with the required CDD requirements. In addition, in case of reliance on foreign third parties, credit intuitions must satisfy themselves that these third parties are based in a jurisdiction that is adequately AML/CFT supervised. If credit institutions rely on intermediaries or other third parties to perform elements of the CDD process, a service level agreement will be required in case the complete CDD process has been outsourced to an intermediary or third party. If the credit institution relies on intermediaries or other third parties for the complete CDD process (in this case the CDD process has been outsourced) then a written service level agreement is required and must be readily available for the Central Bank when conducting onsite visits.
21.	II.2.A. Risk classification	The credit institution must develop risk profiles for all of its customers to determine which categories of customers expose the institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a customer, must take place after the CDD information mentioned above has been received. The risk profile must comprise of minimally the following possible categories: low, medium and high risk. Credit institutions must apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship, or transaction. The credit institutions must at least consider the following risk categories while developing and updating the risk profile of a customer: (i) customer risk, (ii) products/services risk, (iii) country or geographic risk, and (iv) delivery channels risk. The credit institution must make its own determination as to the assignment of the risk weights.

22.	II.2.A. Enhanced Due Diligence	Credit institutions must conduct enhanced due diligence in all of the high risk cases/circumstances and in any other cases/circumstances identified by the institution, according to its risk assessment framework. The institution's decision to enter into or to continue business relationships with such customers must be taken at its senior management level. Credit institutions must not accept or maintain a business relationship if the institution knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations. The credit institution must ensure that the identification documents of its high risk categories of customers are at all times valid.
23.	II.2.A. High-risk and non-cooperative jurisdictions	Credit institutions are required to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations including high-risk and non-cooperative jurisdictions. Banks must exercise special care when their customers have business relations in those countries. If these business relationships and transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions must, as far as possible, be examined, and written findings must be available to assist competent authorities (e.g., supervisors, law enforcement agencies, and the FIU/MOT and auditors). If unusual transactions are detected, then these must be reported to the FIU/MOT.
24.	II.2.A.1 Recognition, documentation, and reporting of unusual transactions	Credit institutions are not only required to adhere to the stipulations of the identification regulations, but they are also required to detect and report either proposed or completed unusual transactions. Therefore, it is important for every institution to have in place adequate procedures for its personnel. Mentioned procedures must cover: (a) the recognition of unusual transactions; (b) the documentation of unusual transactions; and (c) the reporting of unusual transactions.

25.	II.2.A.1. Recognition of unusual transactions	Based on the NORUT legislation, objective and subjective indicators have been established by means of which credit institutions must assess if a customer's transaction qualifies as an unusual transaction. Management must provide its staff with specific guidance and training in recognizing and adequately documenting unusual transactions. Credit institutions must pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.Credit institutions are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. Credit institutions are required to aggregate and monitor balances and activities in customer accounts and apply consistent CDD measures on a fully consolidated worldwide basis, regardless of the type of accounts, such as on- or off balance sheet, and assets under management.
26.	II.2.A.1. Wire transfer	Credit institutions must be extremely vigilant before accepting funds from non-accountholders and non correspondent banks for transfer to equally unknown parties. If such funds are accepted, suitable identification of the non-accountholders and knowledge of the source of funds must be required through a source of funds declaration form. Based on FATF Special Recommendation (SR) VII, credit institutions must include accurate and meaningful originator information (at least the name, address, and account number) regarding funds transfers within or from Curaçao and Sint Maarten, and on related messages sent. The information must remain with the transfer or related message through the payment chain. If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds. Credit institutions must observe the latest Interpretative Note to SR VII and apply its relevant parts. The full text of the Note may be consulted on FATF's website at: **http://ww.fatf-gafi.org**. Also, further scrutiny is required and reporting to the Unusual Transactions Reporting Center (FIU/MOT) must be considered.
27.	II.2.A.1. Correspondent	Credit institutions are not permitted to enter into, or continue, correspondent banking relationships with shell

	banking	banks. Credit institutions are required to satisfy themselves that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks. Particular attention must be paid to correspondent services (such as correspondent banking services) provided to a financial institution licensed in a jurisdiction where the credit institution has no physical presence or is unaffiliated with a regulated bank, or where anti-money laundering and anti-terrorist financing measures and practices are known to be absent and/or inadequate. In addition, the credit institution's policies and procedures regarding the opening of correspondent accounts must at least require the following actions: • fully understand and document the nature of the respondent bank's management and business and determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action; • ascertain that the respondent bank has effective customer acceptance and know-your-customer (KYC) policies and is effectively supervised; and • identify and monitor the use of correspondent accounts that may be used as payable-through accounts. Credit institutions must obtain approval from senior management before establishing new correspondent relationships. Credit institutions establishing correspondent relationships must communicate their documented anti-money laundering and anti-terrorist financing responsibilities to have a clear understanding as to which institution will perform the required measures. Where a correspondent relationship involves the maintenance of "payable-through accounts", credit institutions must be satisfied that: (a) their customer (the respondent financial institution) has performed all the normal CDD obligations on those of its customers that have direct access to the accounts of the correspondent financial institution; and

		(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.
28.	II.2.A.1 Misuse of technological development	Credit institutions are required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.
29.	II.2.A.1. Documentation of unusual transactions	To guard against money laundering and terrorist financing, it is important for credit institutions to provide an audit trail for suspicious funds.
30.	II.2.A.1. Reporting of unusual transactions	Credit institutions must have clear procedures which are communicated to their personnel for the reporting of unusual transactions. The individual transaction or series of transactions which qualify as unusual must be reported internally without undue delay. The designated officers must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU/MOT by the institution, the reasons must be adequately documented and signed off by the compliance officer and/or by management. The designated officers must prepare a report of all unusual transactions for external reporting purposes. The report must be submitted to senior management for their review for compliance with existing regulations and their authorization for submission to the FIU/MOT. Copies of these reports must be kept by the reporting institution. If an unusual transaction is not authorized by senior management to be incorporated in the report to the FIU/MOT, all documents relevant to the transaction including the reasons for non authorization must be adequately documented, signed off by the designated officer and senior management, and kept by the reporting institution. Management must establish a policy to ensure that: - the credit institution and its supervisory directors, senior management, and employees do not warn customers when information about them is being reported to the FIU/MOT, or on internal inquiries

		being made by the institution's compliance staff on customers; and - the institution and its supervisory directors, senior management, and employees follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.
31.	II.2.B. Detection and deterrence of terrorist financing	Credit institutions must take necessary measures to prevent the unlawful use of entities identified as vulnerable, such as charitable or nonprofit organizations, to be used as conduits for criminal proceeds or terrorist financing. Credit institutions must take into account the characteristics including types of transactions listed in the annex 1 to the FATF document entitled "Guidance for Financial Institutions in Detecting Terrorist Financing". In addition, credit institutions must take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities. Supervised institutions must continuously compare the names in their client database with the names on the above-mentioned lists. If a supervised institution encounters a match they must freeze the asset of the client, and report to the FIU/MOT and the Central Bank immediately. If a credit institution suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or by terrorist organizations, it must report promptly its suspicion to the FIU/MOT. Moreover, credit institutions must be vigilant in the abuse of nonprofit organizations for terrorist financing. The institutions must observe the FATF's Special Recommendation (SR) VIII and apply the relevant parts of the FATF document entitled "Combating the abuse of non-profit organizations, International best practices.

32.	II.3	Credit institutions must ensure compliance with the record keeping requirements contained in the relevant money laundering and terrorist financing legislation. Where appropriate, credit institutions must consider retaining certain records relative to unusual transactions of clients for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations. A document retention policy must include the following: • All necessary records on transactions must be maintained for at least five years after the transaction took place. Such records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal behavior. • Records on customer identification, account files and business correspondence must be kept for at least five years after the business relationship has been discontinued. • Credit institutions must ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities. In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure to the FIU/MOT, investigating or law enforcement authority, the records must be retained until it is confirmed by these parties that the case has been closed.
33.	II.2.A.2. Compliance Officer	Each credit institution must formally designate one or more senior officer(s) at management level responsible for the deterrence and detection of money laundering and terrorist financing. The compliance officer(s) must be able to act independently. The AML/CFT compliance officer and other appropriate staff must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The compliance officer must be assigned responsibilities and these must be included in the job description of each designated officer entrusted with the AML/CFT matters. The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.

34.	II.2.A.3. A system of independent testing of policies and procedures	Independent testing of the adequate functioning of the credit institution's policies and procedures must be conducted at least annually by an adequately resourced internal audit department or by an outside independent party, such as the institution's external auditors. The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or to the Board of Supervisory Directors, and to the designated officer(s) with a request to take prompt corrective actions by a certain deadline.
35.	II.2.A.4. Screening of employees/appropriate training plans and program for personnel	Each credit institution must establish and adhere to proper policies and procedures in screening their employees for criminal records. Credit institutions must develop training programs and provide training to all personnel who handle transactions susceptible to the activities listed in the National Decree containing general measures and the Ministerial Decree regarding the Indicators for Unusual Transactions. Training includes setting out rules of conduct governing employees' behavior and their ongoing education to create awareness of the institution's policy against money laundering and terrorist financing. For a credit institution to demonstrate that it has complied with the guidelines with respect to staff training, it must at all times maintain records that include: • details of the content of the training programs provided; • the names of staff who have received the training; • the date on which the training was provided; • the results of any testing carried out to measure staff understanding of the money laundering and terrorist financing requirements; and • an ongoing training plan.

36.	II.4. Examination by the Central Bank	All credit institutions must be prepared to provide information or documentation on money laundering and terrorist financing policies and detection and deterrence procedures to the examiners of the Central Bank before or during an onsite-examination and upon the Central Bank's request during the year.

Money transfer companies (MTCs)

1.	II.2. Policy statement	Each MTCs, Board of Supervisory Directors and senior management must issue a policy statement that expresses the commitment to combat the abuse of its facilities, product and services for the purpose of money laundering and terrorist financing. The policy must state the company's intention to comply with current anti-money laundering and terrorist financing legislation and guidelines, in particular the laws and guidelines regarding the identification of clients and the reporting of unusual transactions. The policy statement must cover also the following items: • The implementation of a formal system of internal control to identify (prospective) clients and deter, detect and report unusual transactions and keep adequate records of the clients and transactions; • The appointment of one or more compliance officers responsible for ensuring day-to-day compliance with these procedures. The officer(s) must have the authority to investigate unusual transactions extensively; • A system of independent testing of the policies and procedures by the MTCs internal audit personnel, compliance department, or by a competent external source to ensure their effectiveness; • The preparation of an appropriate training plan for and training of personnel to increase employees' awareness and knowledge in the area of money laundering and terrorist financing, prevention and detection.
2.	II.2. Detection and deterrence of money laundering	MTCs may only offer their money transfer services to natural persons and have the obligation to identify those (prospective) personal clients/ customers before rendering them money transfer services. Management must maintain an information program to inform those clients of the objectives of the relevant anti-money laundering legislation and inherent requirements for financial institutions. Internal procedures must clearly

		indicate that clients or their representatives must identify themselves and which identification documents are acceptable. The required information must be regularly updated and adequately documented. MTCs must have and follow clear standards on what records must be kept on the aforementioned areas, including individual transactions, and their retention period. An important objective for MTCs is to be able to retrieve this information, without any undue delay.
3.	II.2 Identification checklist	The Central Bank requires the MTC to implement a checklist containing identification and/or transaction information and to maintain a centralized record keeping system to retain copies. The MTCs must ensure that the identification documents are valid at all times.
4.	II.2. Customer Due Diligence	MTCs must develop clear customer policies and procedures with regards to rendering money transfer services, including a description of the types of customers that are likely to pose a higher than average risk to the company. The policy must ensure that transactions will not be conducted with customers who fail to provide satisfactory evidence of their identity.
5.	II.2. Anonymous transfers	Anonymous transfers and fictitious names must be prohibited.
6.	II.2 Ongoing Due Diligence	The efforts to "know your customer" must continue even after the client has been identified. Ongoing due diligence must include also the scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer. If doubts arise relating to the identity of the client after the client has been accepted, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the Financial Intelligence Unit.
7.	II.2. Updated copies of identification document	MTCs must apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer. The required information regarding the client and the allowed identification documents with regards to money transfer services is legally prescribed and must be updated regularly and adequately documented. An important objective for

		MTCs is to be able to retrieve this information, without any undue delay. A MTC must establish the identity of each customer which contemplated or actually performed a money transfer transaction.
8.	II.2. Identification checklist	The implementation of a checklist containing identification and/or transaction information and a centralized record keeping system must be in place. The efforts to "know your customer" must continue once the client has been identified and becomes a regular client.
9.	II.2. Documentation higher risk customers	MTCs are required to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.
10.	II.2. Identification resident and non-resident customers	Pursuant to article 3 of the NOIS, the identity of a **resident** and **non-resident** personal customer must be established through one of the following valid documents: • a driver's license; • an identity card issued; • a travel-document or passport; or • other document to be designated by the Minister of Finance.
11.	II.2. Verification of identity of resident customers	The identity of a **resident** individual customer can be verified by checking a local telephone directory and/or seeking confirmation of identity or activities at other local financial institutions.
12.	II.2. Verification of the identity non-resident customers	MTCs must also pay special attention to non-resident customers and understand the reasons for which the customer uses the company's money transfer services. Verification of the identity of **nonresident** clients must subsequently be obtained by reference to one or more of the following, as deemed practical and appropriate: • international or home country telephone directory; • embassy or consulate in home country of address provided by the prospective client.
13.	II.2.	MTC is bound to establish the identity of the individual

	Identification in case of representation	appearing before him on behalf of a customer or on behalf of a representative of a customer, before it proceeds to render the money transfer service. If the customer acts for a third party or that third party also acts for another third party, the MTC must be bound to also establish the identity of each third party.
14.	II.2. Identification of occasional customers	The procedure for the identification of regular personal customers must also be applied for the identification of occasional personal customers.
15.	II.2. Risk classification	The MTC must develop risk profiles for all of its customers to determine which categories of customers expose the institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a customer, must take place after the CDD information mentioned above have been received. The risk profile must comprise of minimally the following possible categories: low, medium and high risk. MTCs must apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship, or transaction. The MTC must at least consider the following risk categories while developing and updating the risk profile of a customer: (i) customer risk, and (ii) country or geographic risk. The MTC must make its own determination as to the assignment of the risk weights.
16.	II.2. Enhanced Due Diligence	MTCs must conduct enhanced due diligence in all of the high risk cases/circumstances and in any other cases/circumstances identified by the institution, according to its risk assessment framework. The institution's decision to enter into or to continue business relationships with such customers must be taken at its senior management level. MTCs must not accept or provide money transfer services if the institution knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations.

		The MTC must ensure that the identification documents of its customers are at all times valid.
17.	II.2. Identification PEP's	Since all PEPs may not be identified initially as such and existing customers may subsequently obtain a PEP status, MTCs must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, MTCs are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.
18.	II.2.A.1 Identification, verification, and internal control measures for reporting of unusual transactions	MTCs are not only required to adhere to the stipulations of the identification regulations, but they are also required to detect and report either proposed or completed unusual transactions. Hence, it is therefore important for every MTC to have adequate procedures for its personnel in place. These procedures must cover: a. the recognition of unusual transactions; b. the acceptance and documentation unusual transactions; and c. the reporting of unusual transactions.
19.	II.2.A.1. Recognition of unusual transaction	Based on the NORUT, objective and subjective indicators have been established by means of which MTCs must assess if a customer's transaction qualifies as an unusual transaction. Management must provide its staff with specific guidance and training in recognizing and the adequate documenting of unusual transactions. MTCs are required to pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. MTCs are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing.
20.	II.2.A.1. Wire Transfer	MTCs must be extremely vigilant in accepting funds from its customers for transfer. Based on FATF's Special Recommendation (SR) VII, MTCs

		must include accurate and meaningful originator information (at least the receivers and senders name and address) on funds transfers within or from Curaçao and Sint Maarten, and possible related messages that are sent, and the information must remain with the transfer or related message through the payment chain. If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds. Also, further scrutiny is required and reporting to the FIU/MOT must be considered.
21.	II.2.A.1. High-risk and non-cooperative jurisdictions	MTCs must give special attention to transactions involving recipients and senders of funds from high-risk and non-cooperative jurisdictions, being countries that, according to the criteria of FATF, do not apply sufficient anti-money laundering measures and procedures in combating the financing of terrorism. In addition the MTCs policies and procedures must at least require the company to ascertain that the respondent foreign MTC has effective customer and know-your-customer (KYC) policies with respect to rendering money transfer services, and is effectively supervised.
22.	II.2.A.1. Misuse of technological development	MTCs are required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.
23.	II.2.A.1. Documentation of unusual transactions	To guard against money laundering and terrorist financing, it is important for MTCs to provide an audit trail for suspicious funds.
24.	II.2.A.1. Reporting of unusual transactions	MTCs must have clear procedures which are communicated to their personnel for the reporting of unusual transactions. The individual transaction or series of transactions which qualify as unusual must be reported internally without any undue delay. The designated officers must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU/MOT by the compliance officer, the reasons therefore must be adequately documented and signed off by this officer

		and/or by management. The designated officers must prepare a report of all unusual transactions for external reporting purposes. The report must be submitted to senior management for their review for compliance with existing regulations and their authorization for submission to the Unusual Transactions Reporting Center (MOT). Copies of these reports must be kept by the reporting MTC. If an unusual transaction is not authorized by senior management to incorporate in the report to the FIU/MOT all documents relevant to the transaction including the reasons for non-authorization must be adequately documented, signed off by the designated officer and senior management and kept by the reporting MTC. Management must establish a policy to ensure that: • the MTC and its Supervisory Directors, senior management and employees do not warn customers when information about them is being reported to the FIU/MOT, or on internal inquiries being made by the institution's compliance staff on them; • the MTC and its Supervisory Directors, senior management and employees follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.
25.	II.2.B. Detection and deterrence of terrorist financing	MTCs must take into account the relevant characteristics including types of transactions listed in the annex 1 to the FATF document:"Guidance for Financial Institutions in Detecting Terrorist Financing". In addition, MTCs must take into account other available information including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities. Supervised institutions must continuously match their client's database with the names on the above-mentioned lists. If a supervised institution encounters a match they must freeze the asset of the client and inform the Central Bank immediately. If a MTC suspects or has reasonable grounds to suspect that

		funds are linked or related to, or are to be used for terrorism, terrorist acts, or by terrorist organizations, it must report promptly its suspicion to the FIU/MOT. Moreover, MTCs must be vigilant in the abuse of nonprofit organizations for terrorist financing. The institutions must observe the FATF's Special Recommendation (SR) VIII and apply the relevant parts of the FATF document entitled "Combating the abuse of non-profit organizations, International best practices.
26.	II.2.B. Record keeping	MTCs must ensure compliance with the record keeping requirements contained in the relevant money laundering and terrorist financing legislation. Where appropriate, MTCs must consider retaining certain records e.g. customer identification, account files, business correspondence, and internal and external reports relative to unusual transactions of clients for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations. A document retention policy must include the following: • All necessary records on transactions (both domestic and international) must be maintained for at least five years after the transaction tokes place. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts, currencies, and type of transaction involved) so as to provide, if necessary, evidence for prosecution of criminal behavior. • Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship has been discontinued. • MTCs must ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities. In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure to the FIU/MOT, investigating or law enforcement authority, they must be retained until it is

		confirmed by these parties that the case has been closed.
27.	II.2.A.2. Compliance Officer	Each MTC must formally designate one or more officer(s) at management level responsible for the deterrence and detection of money laundering and terrorist financing. The compliance officer(s) must be able to act independently. The AML/CFT compliance officer and other appropriate staff must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The compliance officer(s) must be assigned responsibilities and these must be included in the job description of each designated officer. The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.
28.	II.2.A.3. A system of independent testing of policies and procedures	Independent testing of the adequate functioning of the MTCs policies and procedures must be conducted at least annually by an adequately resourced internal audit department or by an outside independent party such as the MTCs external auditors. The scope of the testing and of the results must be documented, with any deficiencies being reported to senior management and/or to the Board of Supervisory Directors, and to the designated officers with a request for a response indicating corrective action taken or to be taken and a deadline for doing so.
29.	II.2.A.4. Screening of employees/appropriate training plans and program for personnel	Each company must establish and adhere to proper policies and procedures to screen their employees on criminal records. MTCs must at a minimum develop training programs and provide training to all personnel who handle transactions susceptible to the activities listed in the National Decree containing general measures and the Ministerial Decree regarding the Indicators for Unusual Transactions. Training includes setting out rules of conduct governing employees' behavior and their ongoing education, in order to create awareness for the MTCs policy against money laundering and terrorist financing. For a MTC to demonstrate that it has complied with the aforementioned guidelines with respect to staff training, it

		must at all times maintain records that include: • the names of staff who have received the training; • details of the content of the training programs provided; • the date on which the training was provided; • the results of any testing carried out to measure staff understanding of the money laundering and terrorist financing requirements; and • an ongoing training plan.
30.	II.3. Examination by the Central Bank	All MTCs must be prepared to provide information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the Central Bank before or during an onsite examination, and upon the Central Bank's request during the year.

Company (Trust) Service Providers

1.	II.2. Policy statement	The Board of Directors and senior management of a company service provider must issue a policy statement that clearly expresses the commitment of the company service provider to combat the abuse of the company service provider's facilities and services for the purpose of money laundering and terrorist financing. The obligation to issue a policy statement is also applicable to a natural person that provides trust services to international companies. The policy must state the intention of the company service provider to comply with current anti-money laundering and terrorist financing legislation as well as provisions and guidelines, in particular the laws and guidelines regarding the identification of clients and the reporting of unusual transactions. The policy statement also must cover the following items: - The implementation of a formal system of internal control to identify (prospective) clients, deter, detect, and report unusual transactions, and keep adequate records of the clients and transactions. - The preparation of an appropriate training plan for and the training of personnel of a company service provider that is a legal person or for the company service provider who is a natural person to increase awareness and knowledge in the area of money laundering and terrorist financing prevention and detection. - The appointment of one or more compliance officers at management level, responsible for ensuring the day-to-day compliance with these procedures. The officer must have the authority to investigate unusual transactions extensively. If the company service provider is a natural person, this natural person must be entrusted with the compliance function.

		- A system of independent testing of the policies and procedures by the company service provider's internal audit personnel or by a competent external source to ensure their effectiveness. - the company service provider and, in case it is a legal entity, also its directors, officials and employees must not warn their clients when information about them is being reported to the FIU/MOT, or on internal inquiries being made by (the compliance staff of) company (trust) service provider on them; - the company (trust) service provider and, in case it is a legal entity, its directors, officials and employees must follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.
2.	II.2.A. Detection and deterrence of money laundering	Company (trust) service providers have the obligation to identify their (prospective) clients/customers, including, where applicable, the (ultimate) beneficiaries of their prospective clients/customers, before rendering them their services. Company (trust) service providers must maintain an information program to inform those clients of the objectives of the relevant anti-money laundering legislation and inherent requirements for company (trust) service providers. The internal procedures of a company service provider must clearly indicate for which services clients or their representatives must identify themselves and which identification documents are acceptable. The required information must be regularly updated and adequately documented. Company

		(trust) service providers must have and follow clear standards on what records must be kept on the aforementioned areas, including individual transactions, account files and business correspondence and on their retention period for current as well as terminated business relationships. An important objective for company (trust) service providers is to be able to retrieve this information, without any undue delay.
3.	II.2.A.Identification checklist	The Central Bank requires the company service provider to implement a checklist containing identification and/or transaction information, and to maintain a centralized record keeping system to retain copies. Company (trust) service providers must ensure that the identification documents are valid at all times.
4. 4.	II.2.A. Policies and procedures Non-face-to-face business relationship	Company service providers must have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. These policies and procedures must apply when establishing customer relationships and when conducting ongoing due diligence.
5.	II.2.A. Customer Due Diligence	Before the provision of trust services to a client, identification of a prospective client must be made from documents issued by reliable sources as prescribed in the NOIS and whenever applicable/possible the directors, representatives or Ultimate Beneficial Owners of the prospective client must be interviewed personally. Company (trust) service providers are also required to obtain and document information on the purpose and intended nature of the business relationship with their (prospective) clients prior to offering them their services.
6.	II.2.A. Ongoing Due Diligence	The efforts to "know your customer" must continue once the client has been identified, even after the initial identification of the client. While the on-going due diligence process must also

		include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the company service provider's knowledge of the client, its business and risk profile, and where necessary, the source of funds. In the event that doubts relating to the identity of the client arise after the client has been accepted, the relationship with the client must be re-examined to determine whether it must be terminated and whether the incident must be reported to the Financial Intelligence Unit (FIU).
7.	II.2.A. Updated copies of identification document	Company (trust) service providers must apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. Updated copies of the identification document must be retained if the company service provider becomes aware that it lacks sufficient information about an existing customer. The company service provider must ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of clients or business relationships.
8.	II.2.A. Identification of face-to-face business relationship	When providing face to face business relationships or transactions a company service provider must: • provide the original transaction document with the text: "Mr. and or Mrs. ……. appeared to me in person"; and a stamp with the prevailing date; and • add the signature of the client and the employee who performed the transaction to the original transaction document.
9.	II.2.A. Identification of (prospective) clients	Therefore, the company (trust) service provider must look beyond the international company for due diligence purposes and, depending upon the circumstances, requests proof of identity of any of the following parties:

		• the (managing and supervisory) directors of the international company; • the (ultimate) beneficial owners or beneficiaries of the international company; • in case any of the parties mentioned above is a legal entity, the directors of and the (ultimate) beneficial owners holding a qualifying interest in the legal entity. Please note that a proof of registration of the legal entity with the Chamber of Commerce and Industry, or an equivalent institution, in the country of domicile must also be requested. Pursuant to article 3 of the NOIS, the identity of the parties (whether resident or non-resident) must be established through one of the following valid documents: • a driver's license; • an identity card issued; • a travel document or passport; • other document to be designated by the Minister of Finance.
10.	II.2.A. Verification identity of resident customers	The identity of a **resident** individual must be verified when a business relationship is established with the international company. The identity of a resident individual that has previously been subject to the company service provider's CDD must also be verified when the company service provider has doubts about the veracity or adequacy of the identification data obtained in the past in this individual.
11.	II.2.A. Identification Non-resident customers	For **nonresident** individuals a copy of the identifications document is sufficient, under the condition that the relevant document is accompanied by a certified extract of the civil registry of births, marriages and deaths of the place of residence of the party or that the document is certified by a notary public or embassy/consulate.

12.	II.2.A. Verification of the identity non-resident customers	The company service provider must verify the existence and nature of the international company's business through reliable identification documents, with preference for originals and official documents. The existence and nature of a (prospective) international company must be legally identified with the aid of a certified extract from the register of the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation, or with the aid of an identification document to be drawn up by the company service provider. The extract or the identification document must contain at least the information stipulated by the Minister of Finance. The name, address and telephone number of the notary public/professional/institution including the name and contact details of the institution's officer who actually signed for verification must be clearly indicated. Furthermore, the submitted copy of the identification document, including the photograph, must be clearly legible.
13.	II.2. A. Identification of PEP's	Company (trust) service provider s must conduct enhanced due diligence for politically exposed persons (PEPs), their families and associates. The institution's decision to enter into business relationships with PEPs must be taken at its senior management level. The institution must make reasonable efforts to ascertain that the PEP's source of wealth and source of funds/ income is not from illegal activities and where appropriate, review the customer's credit and character and the type of transactions the customer would typically conduct. Company (trust) service provider s must not accept or maintain a business relationship if the institution knows or must assume that the funds are derived from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, financial institutions must obtain senior management approval to continue the business relationship. Where the financial institution is in a

		business relationship with a PEP, they must conduct enhanced ongoing monitoring on that relationship.
14.	II.2.A. Identification of nominee shareholders	All company (trust) service providers that provide nominee shareholder services and/or provide custody of bearer shares must know the true identity of the person/persons (resident or non-resident) for whom assets are held or are to be held, including the (ultimate) beneficial owner(s). The identity of these clients must be established in accordance with the identification procedures.
15.	II.2.A. Anonymous accounts	Anonymous accounts or accounts in fictitious names are prohibited.
16.	II.2.A. Numbered accounts	Where numbered accounts are opened by the company service provider on behalf of its clients, the company service provider is required to maintain this account in such a way that full compliance can be achieved with the FATF Recommendations.
17.	II.2.A. Bare trust (fixed trust)/ Discretionary trust	Where the trust is identified as a bare or fixed trust it is the settler that must be identified as the person exercising effective control over the trust and the trustees as the ultimate beneficiaries of the trust. Therefore, CDD measures must be applied to both the trustee, being the ultimate beneficiary, and the settler of the trust. Where the trust is identified as a discretionary trust the ultimate beneficiary is not previously established. In this case a distinction must be made between applicable CDD measures at time of establishing the trust and CDD measures applicable at the time of appointment of beneficiaries of the trust. When the trust is established and thereby the client relationship is created, in case of a discretionary trust, CDD measures apply to the settler of that trust. As soon as the beneficiaries of the trust are appointed, the company service provider is required to perform proper CDD on

		the beneficiary (ies).
18.	II.2.A. Reliance on intermediaries or other third parties	If company (trust) service providers rely on intermediaries or other third parties to perform some of the elements of the CDD process or to introduce business, they must take the following steps: • immediately obtain from the third party the necessary information concerning the performed elements of the CDD process; • take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay, however, not longer than within a timeframe of 24 hours; • satisfy themselves that the third party is AML/CFT regulated and supervised, and has measures in place to comply with the required CDD requirements; • in determining in which countries the third party that meets the conditions can be based, company (trust) service providers must take into account information available on whether those countries adequately apply the FATF Recommendations. In addition, in case of reliance on foreign third parties, credit intuitions must satisfy themselves that these third parties are based in a jurisdiction that is adequately AML/CFT supervised. If company service provider rely on intermediaries or other third parties to perform elements of the CDD process, a service level agreement will be required in case the complete CDD process has been outsourced to an intermediary or third party. If company (trust) service providers rely on intermediaries or other third parties to perform the elements of the CDD process, a service level agreement will be required in case the complete

		CDD process has been outsourced to an intermediary or other third party.
19.	II.2.A. Risk classification	The company service provider must develop risk profiles for all of its customers to determine which categories of clients expose the institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a client, must take place after the CDD information mentioned above has been received. The risk profile must comprise of minimally the following possible categories: low, medium and high risk. Company (trust) service providers must apply CDD requirements to existing clients and may determine the extent of such measures on a risk sensitive basis depending on the type of client, business relationship, or transaction. Company (trust) service providers must at least consider the following risk categories while developing and updating the risk profile of a client: (i) customer risk, (ii) products/services risk, (iii) country or geographic risk, and (iv) delivery channels risk The company service provider must make its own determination as to the assignment of the risk weights.
20.	II.2.A. Enhanced Due Diligence	Company (trust) service providers must conduct enhanced due diligence for high risk customers, including politically exposed persons (PEPs), their families and associates, and (internet) gambling businesses. The company service provider's decision to enter into business relationships with such clients must be taken at its senior management level. Company (trust) service providers must not accept or maintain a business relationship if the company (trust) service provider knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law

		or other laws or regulations. The company service provider must develop risk profiles to determine which of the categories expose the company service provider to higher risk. The company (trust) service provider must ensure that the identification documents of its high risk categories of customers are at all times valid.
21.	II.2.A. Identification PEP's	Since all PEPs may not be identified initially as such and existing customers may subsequently obtain a PEP status, company (trust) service providers must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, company (trust) service providers are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.
22.	II.2.A. High risk and non-cooperative jurisdictions	Company (trust) service providers are required to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF Recommendations including the high-risk and non-cooperative jurisdictions. Company (trust) service providers must exercise special care when their customers have business relations in those countries. If these business relationships and transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions must, as far as possible, be examined, and written findings must be available to assist competent authorities (e.g. supervisors, law enforcement agencies and the FIU/MOT and auditors). If unusual transactions are detected, then these must be reported to the FIU/MOT.
23.	II.2.A.1. Identification, verification and internal control measures for reporting of unusual	Company (trust) service providers are not only required to adhere to the stipulations of the identification regulations, but they are also required to detect and report either proposed or

	transactions	completed unusual transactions. Hence, it is therefore important for every company service provider to have adequate procedures for its personnel in place. These procedures must cover: (a) the recognition of unusual transactions; (b) the documentation of unusual transactions; and (c) the reporting of unusual transactions.
24.	II.2.A.1. Recognition of unusual transaction	Company (trust) service providers are required to pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. Company (trust) service providers are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. The company service provider must provide its staff with specific guidance and training to recognize and document adequately the unusual transactions.
25.	II.2.A.1. Wire transfer	Company (trust) service providers must be extremely vigilant when proceeds are transferred from or to accounts with financial institutions licensed in jurisdictions where anti-money laundering measures and practices are known to be absent and/or inadequate. Based on FATF Special Recommendation (SR) VII, company (trust) service providers must include accurate and meaningful originator information (at least the name, address and account number if existent, otherwise a unique reference number) on funds transfers on behalf of their clients within or from Curaçao and Sint Maarten and related messages that are sent. If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds. Company (trust) service providers must observe

		the latest Interpretative Note to SR VII and apply its relevant parts. Also, further scrutiny is required and reporting to the FIU/MOT must be considered.
26.	II.2.A.1. Misuse of technological development	Company (trust) service provider s are required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.
27.	II.2.A.1. Documentation of unusual transactions	To guard against money laundering and terrorist financing, it is important for company (trust) service provider s to provide an audit trail for suspicious funds.
28.	II.2.A.1. Reporting of unusual transactions	Company (trust) service providers must have clear procedures which are communicated to their personnel for the reporting of unusual transactions. The obligation to report internally, without any undue delay, lies on anyone who renders financial services by virtue of his profession or in the ordinary course of his business. The designated officer(s) must keep an adequate filing system for these records. If internally reported transactions are not reported to the FIU/MOT by the compliance officer or the person responsible for the compliance function, the reasons therefore must be adequately documented and signed off by this person and/or by management. A report must be prepared of all unusual transactions by the designated officer(s) for external reporting purposes. Company (trust) service providers that are natural persons also have the obligation to send the report to the FIU/MOT. All company (trust) service providers must keep copies of all reports submitted to the FIU/MOT on file.

		If an unusual transaction is not authorized by senior management to be incorporated in the report to the FIU/MOT, all documents relevant to the transaction including the reasons for non-authorization must be adequately documented, signed off by the designated officer and senior management and kept by the reporting institution. If existing, non-executive (supervisory) directors must be notified in case the officer disagrees on the absence of above-mentioned authorization. In this respect, all documents relevant to the case and motivations must be submitted for further notification to the non-executive (supervisory) directors within three business days after the non-authorization, including any individual further exposition on the case by each designated officer and/or senior management. Each individual exposition must also be kept by the reporting institution.
29.	II.2.B. Detection and deterrence of terrorist financing	Company (trust) service providers must take into account the characteristics including types of transactions listed in annex 1 to the FATF document "Guidance for Financial Institutions in Detecting Terrorist Financing". Those characteristics and transactions could be a reason for additional scrutiny and could indicate funds involved in terrorist financing. In addition, company (trust) service providers must take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities. Supervised institutions must continuously match their client's database with the names on the above-mentioned lists. If a supervised institution encounters a match they must freeze the asset of the client and inform the Central Bank immediately. In addition, company (trust) service providers

		must be vigilant in the abuse of non-profit organizations for terrorist financing. They must observe the FATF's Special Recommendation (SR) VIII. If company (trust) service providers suspect or have reasonable grounds to suspect that funds of the international company and/or its related party are linked or related to, or are to be used for terrorism, terrorist acts, or by terrorist organizations, they must report promptly their suspicion to the FIU/MOT.
30.	II.2.B. Record keeping	Company (trust) service providers must ensure compliance with the record keeping requirements contained in the relevant money laundering and terrorist financing legislation. Where appropriate, company (trust) service providers must consider retaining certain records e.g. customer identification, account files, business correspondence, and internal and external reports relative to unusual transactions of clients for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations. A document retention policy must include the following: • All necessary records on transactions (both domestic and international) must be maintained for at least five years after the transaction takes place. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts, currencies, and type of transaction involved) so as to provide, if necessary, evidence for prosecution of criminal behavior. • Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the business relationship has been discontinued.

		• Company (trust) service providers must ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities. In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure to the FIU/MOT, investigating or law enforcement authority, they must be retained until it is confirmed by these parties that the case has been closed.
31.	II.2. A.2.Compliance officer	Each company service provider must formally designate one or more officer(s) at management level, responsible for the deterrence and detection money laundering and terrorist financing. If the company (trust) service provider is a natural person, this natural person must be entrusted with the compliance function. The compliance officer(s) or natural person must be assigned responsibilities and these must be included in the job description of the designated officer entrusted with the company service provider's anti-money laundering and terrorist financing matters. The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.
32.	II.2.A.3. A system of independent testing of policies and procedures	The independent testing must be conducted at least annually by the internal audit department or by an outside independent party, such as the external auditor of the company (trust) service provider. The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or to the Board of Directors, and to the designated officer(s) with a request to take prompt corrective actions by a certain deadline.
33.	II.2.A.4. Screening of employees/appropriate training plans and program for personnel	Company (trust) service providers must ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed. Each company (trust) service provider that has a

		staff must screen its employees on criminal records. Company (trust) service providers must develop training programs and provide training to all personnel who handle transactions susceptible to the activities listed in the National Decree containing general measures and the Ministerial Decree regarding the Indicators for Unusual Transactions. The training must include a clear explanation of all aspects of the laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification and due diligence. In order for a company (trust) service provider to be able to demonstrate that it has complied with the aforementioned guidelines with respect to training, it must at all times maintain records which include: • details of the content of the training programs provided (for company (trust) service providers that are legal persons) or training programs followed (for company (trust) service providers that are natural persons); • the names of the person(s) who have received the training; • the date on which the training was provided; • the results of any testing carried out to measure the participants' understanding of the money laundering and terrorist financing requirements; and • an on-going training plan.
34.	II.3 Examination by the Central Bank	All company service providers must be prepared to provide information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the Central Bank before or during an examination and upon the Central Bank's request during the year.

1.	II Provisions & Guidelines AML & CFT	The Central Bank requires all investment institutions that have outsourced their administrative tasks to an administrator, to clearly indicate in an agreement that the administrator will adhere to the laws and regulations related to money laundering and terrorist financing applicable to the investment institution while carrying out its administrative duties for the investment institution. This contract must be signed by both the investment institution and the administrator.
2.	II.2. Policy statement	The Board of Directors and senior management of a administrator or of a self-administered investment institution must issue a policy statement, which clearly expresses the commitment of the administrator and self-administered investment institution to combat the abuse of its facilities and services for the purpose of money laundering and terrorist financing. The policy must state the intention of the administrator and self-administered investment institution to comply with current anti-money laundering and terrorist financing legislation and guidelines, in particular the laws and guidelines regarding the identification of clients and the reporting of unusual transactions. The policy statement must cover also the following items: • The implementation of a formal system of internal control to identify (prospective) clients and deter, detect and report unusual transactions and keep adequate records of the clients and transactions; • The appointment of one or more compliance officers responsible for ensuring day-to-day compliance with these procedures. The officer(s) must have the authority to investigate unusual transactions extensively; • A system of independent testing of the policies and procedures by the institution's internal audit personnel, compliance department, or by a competent external source to ensure their effectiveness; • The preparation of an appropriate training program for personnel to increase employees' awareness and

		knowledge in the area of money laundering and terrorist financing prevention and detection.
3.	II.2.A. Detection and deterrence of money laundering	Administrators and self-administered investment institutions must have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. They must also have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions. These policies and procedures must apply when establishing customer relationships and when conducting ongoing due diligence.
4.	II.2.A. Identification of face-to-face business relationship	When providing face to face business relationships or transactions a company service provider must: • provide the original transaction document with the text: "Mr. and or Mrs. ……. appeared to me in person"; and a stamp with the prevailing date; and • add the signature of the client and the employee who performed the transaction to the original transaction document.
5.	II.2.A. Customer Due Diligence	Administrators have the obligation to determine the true identity, including the (ultimate) beneficiaries of their (prospective) clients, where applicable, before offering them administrative services. Administrators are also required to obtain information on the purpose and intended nature of the business relationship with their (prospective) clients prior to offering them administrative services. Internal procedures must also clearly indicate which identification documents are required for the acceptance of prospective clients. The required information regarding the (prospective) client, the authorized identification documents and the nature of the administrative service(s) to be provided must be adequately described and documented. An important objective for administrators is to be able to retrieve this information, when needed, without any undue delay.

6.	II.2.A. Identification checklist	The implementation of a checklist containing the identification and/or information of clients to which administrative services are provided and a centralized record keeping system must be in place.
7.	II.2.A. Ongoing Due Diligence	The execution of the "know your customer" policy must be a continuous process, even after the initial identification of the client. The continuous process must include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the administrator's knowledge of the client, its business and risk profile, and the source of funds.
8.	II.2.A. Source of funds declaration form	It is a compulsory requirement for administrators to fill out the Source of Funds Declaration Form.
9.	II.2.A. Client acceptance policy	Administrators must develop clear client acceptance policies and procedures, including a description of the types of client that are likely to pose a higher than average risk to them. The policy must ensure that the administrator will not provide administrative services to clients who fail to provide satisfactory evidence of their identity.
10.	II.2.A. Identification of PEP's	Administrators must conduct more extensive due diligence for high risk clients, including politically exposed persons ("PEPs"), families and associates of PEPs. The administrator's decision to enter into business relationships with such clients must be taken at its senior management level. The administrator must make reasonable efforts to ascertain that the client's source of wealth or income is not from illegal activities. Additionally, administrators and self-administered institutions are encouraged to conduct enhanced ongoing monitoring on PEPs who hold prominent public functions domestically.
11.	II.2.A. Updated copies of identification document	Administrators must be required to ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of clients or business relationships.

		Administrators must not accept or maintain a business relationship if the administrator knows or must assume that the funds of the client were derived from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations.
12.	II.2.A. Reliance on intermediaries or other third parties	These steps must be taken by administrators and self-administered institutions when relying on intermediaries or other third parties to perform aforementioned elements of the CDD process: • immediately obtain from the third party the necessary information concerning the elements of the CDD process; • satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay; • satisfy themselves that the third party is AML/CFT regulated and supervised, and has measures in place to comply with the required CDD requirements. In addition, in case of reliance on foreign third parties, administrators and self-administered institutions must satisfy themselves that these third parties are based in a jurisdiction that is adequately AML/CFT supervised. If administrators and self-administered institutions rely on intermediaries or other third parties to perform elements of the CDD process, a service level agreement will be required in case the complete CDD process has been outsourced to an intermediary or third party. In case only one or two elements of the due diligence process is/are performed by an intermediary or third party (like for example identifying the client and verifying the copy of a passport) then a service level agreement is not required. In case the administrators and self-administered institutions rely on other third parties for the complete CDD process (in this case the CDD process has been outsourced) than a written contractual arrangement is

		required and must be readily available for the Central Bank when conducting onsite visits.
13.	II.2.A. Identification of (prospective) clients	The administrator must look beyond the investment institution for due diligence purposes and, depending upon the circumstances, requests proof of identity of any of the following parties: • the (managing and supervisory) directors of the investment institution; • any party who provides or will provide instructions to the administrator on behalf of the investment institution; • in case any of the parties mentioned above is a legal entity, the directors and the ultimate beneficial owners holding a qualifying interest in the legal entity. Please note that a proof of registration of the legal entity with the Chamber of Commerce and Industry, or an equivalent institution, in the country of domicile must also be requested. Pursuant to article 3 of the NOIS, the identity of the parties must be established through one of the following valid documents: • a driver's license; • an identity card issued: • a travel document or passport; and • any other document designated by the Minister of Finance.
14.	II.2.A. Verification (prospective) identification	The administrator must verify the existence and nature of the investment institution's business through reliable identification documents, with preference for originals and official documents. The existence and nature of a (prospective) investment institution must be legally identified with the aid of a certified extract from the register of the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation, or with the aid of an identification document to be drawn up by the administrator. The extract or the identification document must contain at least the information stipulated by the Minister of Finance.
15.	II.2.A.	Investment institutions have the obligation to

	Due Diligence on (prospective) investors	determine the true identity of their (prospective) investors, including where applicable the (ultimate) beneficiaries of their investors that are legal entities. Administrators and self-administered investment institutions are required to obtain information on the purpose and intended nature of the business relationship with their (prospective) investors. The internal policies and procedures of the administrator and the self-administered investment institution must clearly describe which identification documents are acceptable for the acceptance of investors in the (self-) administered investment institution. These policies and procedures must also include a description of the types of investor that are likely to pose a higher than average risk to the investment institution. These policies and procedures must ensure that (prospective) investors will not be accepted in case they fail to provide satisfactory evidence of their identity. Administrators and self-administered investment institutions must also be able to retrieve the information received from investors, when needed, without any undue delay.
16.	II.2.A. Identification checklist	The implementation of a checklist containing the identification and/or transaction information of investors and a centralized record keeping system must be in place.
17.	II.2.A. Ongoing Due Diligence investor	The execution of the "know your customer" policy must be a continuous process, even after the initial identification of the investor. The continuous process must include scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the administrator's and self administered investment institution's knowledge of the investor, its source of funds, and its (business and) risk profile.
18.	II.2.A. Enhanced Due Diligence (investor)	Administrators and self-administered investment institutions must conduct more extensive due diligence for high risk investors, including politically exposed persons (PEPs), families and associates of PEPs. The decision to accept such investors must be taken at senior management level. The administrator and self-

		administered investment institution must make reasonable efforts to ascertain that such high risk investor's source of wealth or income is not from illegal activities. The administrator and self-administered investment institution must not accept or maintain a business relationship with an investor if the administrator knows or has reasonable grounds to believe that the funds were derived from corruption or misuse of public assets, without prejudice to any obligation the administrator and self-administered investment institution has under criminal law or other laws or regulations.
19.	II.2.A. Identification of PEP's (investor)	Since all PEPs may not be identified initially as such and existing customers may subsequently obtain a PEP status, administrators and self-administered investment institution must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, administrators and self-administered investment institutions are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.
20.	II.2.A. Updated copies of identification document (investor)	Administrators and self-administered investment institutions are required to ensure that documents, data or information collected under the due diligence process relative to the investor is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of investors.
21.	II.2.A. Preventive measures	Administrators and self-administered investment institution must take necessary measures in preventing the unlawful use of entities identified as vulnerable, such as charitable or non-profit organizations, to be used as conduits for criminal proceeds or terrorist financing.
22.	II.2.A. Identification at time of subscription	All (prospective) investors must be duly identified at the time of subscription in the investment institution. The efforts to "know your customer" must continue once the client has been identified. For identity purposes, the following categories of investors are distinguished:

		A) investor is a financial institution; B) investor is an individual; C) investor is a partnership; D) investor is a corporate entity; E) investor is a corporation which is a private company; F) investor is an institutional investor.
23.	II.2.A. Exemption on identification of investor	Administrators and self-administered investment institutions must document in their records the reason why no further identification documents were requested from the investor.
24.	II.2.A. Bearer shares	The financial service providers in Curaçao and Sint Maarten must always know the beneficial owners of bearer shares of companies to whom it renders services, which are not listed on a public securities exchange. Certificate of bearer shares must be held in custody by the administrator or self-administered investment institution or a party assigned by the administrator or self-administered investment institution.
25.	II.2.A. Risk classification	The administrator and self-administered investment institution must develop risk profiles for all of its clients, being investment institutions and/or investors, to determine which categories of clients expose the administrator and self-administered investment institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the preparation of the risk classification of a client, must take place after the CDD information mentioned above has been received. The risk profile must comprise of minimally the following possible categories: low, medium and high risk. Administrators and self-administered investment institutions must apply CDD requirements to existing clients and may determine the extent of such measures on a risk sensitive basis depending on the type of client, business relationship, or transaction. Administrators and self-administered investment institutions must at least consider the following risk categories while developing and updating the risk profile of a client: (i) client risk, (ii) products/services risk, (iii) country or geographic risk, and (iv) delivery channels risk.

		The administrator and self-administered investment institution must make its own determination as to the assignment of the risk weights.
26.	II.2.A. Enhanced Due Diligence	Administrators and self-administered investment institutions must conduct enhanced due diligence in all of the high risk cases/circumstances mentioned above and in any other cases/circumstances identified by the institution, according to its risk assessment framework. The institution's decision to enter into or to continue business relationships with such customers must be taken at its senior management level. Administrators and self-administered investment institutions must not accept or maintain a business relationship if the institution knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations. The Administrators and self-administered investment institutions must ensure that the identification documents of its high risk categories of customers are at all times valid.
27.	II.2.A. Identification of PEP's	Since all PEPs may not be identified initially as such and existing customers may subsequently obtain a PEP status, administrators and self-administered investment institutions must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, administrators and self-administered investment institutions are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.
28.	II.2.A. High-risk and non-cooperative jurisdictions	Administrators and self-administered investment institutions are required to give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations including high-risk and non-cooperative jurisdictions. If these business relationships and transactions have no apparent economic or visible lawful purpose, the background and

		purpose of such transactions must, as far as possible, be examined, and written findings must be available to assist competent authorities (e.g., supervisors, law enforcement agencies, and the FIU/MOT and auditors). If unusual transactions are detected, then these must be reported to the FIU/MOT.
29.	II.A.2.1. Identification, verification, and internal control measures for reporting of unusual transactions	Administrators and self-administered investment institutions are not only required to adhere to the stipulations of the identification regulations, but they are also required to detect and report either proposed or completed unusual transactions. Hence, it is therefore important for every administrator and self-administered investment institution to have adequate procedures for its personnel in place. These procedures must cover: (a) the recognition of unusual transactions; (b) the acceptance and documentation of unusual transactions; and (c) the reporting of unusual transactions.
30.	II.2.A.1. Recognition of unusual transaction	Administrators and (self-) administered investment institutions are required to pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. Administrators and (self-) administered investment institutions are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. Management must provide its staff with specific guidelines and training to recognize and document adequately the unusual transactions.
31.	II.2.A.1. Wire transfer	Based on FATF Special Recommendation (SR) VII, administrators and self-administered investment institutions must be extremely vigilant when proceeds are transferred from or to accounts with financial institutions licensed in jurisdictions where anti-money laundering measures and practices are known to be absent and/or inadequate. Administrators and self-administered investment

		institutions must include accurate and meaningful originator information (at least the name, address and account number) on funds transfers within or from Curaçao and Sint Maarten, and related messages that are sent. The information must remain with the transfer or related message through the payment chain. If the information seems inaccurate or incomplete, additional information must be requested prior to accepting or releasing funds. Also, further scrutiny is required and reporting to the Unusual Transactions Reporting Center (FIU/MOT) must be considered.
32.	II.2.A.1. Documentation of unusual transactions	To guard against money laundering and terrorist financing, it is important for administrators and self-administered investment institutions to provide an audit trail for suspicious funds.
33.	II.2.A.1. Reporting of unusual transactions	Administrators and self-administered investment institutions must have clear procedures which are communicated to their personnel for the reporting of unusual transactions. All transactions in the list of indicators of the National Ordinance on the Reporting of Unusual Transactions, must be referred to the designated officer(s), in a format which contains at least the data as stipulated by law. The designated officer(s) must keep an adequate filing system for these records. If internally reported transactions are not reported to the FIU/MOT by the compliance officer, the reasons therefore must be adequately documented and signed off by this officer and/or by management. A report must be prepared of all unusual transactions by the designated officer(s) for external reporting purposes. The report must be submitted to senior management for review of compliance with existing regulations. The administrator must keep copies of all reports submitted to the FIU/MOT on file. If an unusual transaction is not authorized by senior management to be incorporated in the report to the

		FIU/MOT, all documents relevant to the transaction including the reasons for non-authorization must be adequately documented, signed off by the designated officer and senior management and kept by the reporting institution. In addition, in case the officer disagrees on the absence of the authorization, all documents relevant to the case and motivations must be submitted for further notification to the Board of Directors within three business days after the non-authorization, including any individual further exposition on the case by each designated officer and/or senior manager. Each individual exposition must also be kept by the reporting institution. Management must establish a policy to ensure that: - the administrator or self-administered investment institution and its directors, officials and employees do not warn their clients when information about them is being reported to the FIU/MOT, or on internal inquiries being made by the compliance staff of the administrator or self-administered investment institution on them; - the administrator or self-administered investment institution and its directors, officials and employees follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.
34.	II.2.B. Detection and deterrence of terrorist financing	Administrators and self-administered investment institutions must take into account the characteristics including types of transactions listed in the annex 1 to the FATF document "Guidance for Financial Institutions in Detecting Terrorist Financing". In addition, administrators and self-administered investment institutions must take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities. Supervised institutions must continuously compare the names in their client database with the names on the above-mentioned lists. If a supervised institution encounters a match they must freeze the asset of the

		client, and report to the FIU/MOT and the Central Bank immediately. If they suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or by terrorist organizations, they must report promptly their suspicion to the FIU/MOT. Moreover, administrators and self-administered investment institutions must be vigilant in the abuse of nonprofit organizations for terrorist financing. The institutions must observe the FATF's Special Recommendation (SR) VIII and apply the relevant parts of the FATF document entitled "Combating the abuse of non-profit organizations, International best practices.
35.	II.2.B. Record keeping	Administrators and self-administered investment institutions must ensure compliance with the record keeping requirements contained in the relevant money laundering and terrorist financing legislation. Where appropriate, administrators must consider retaining certain records e.g. customer identification, account files, and business correspondence, and internal and external reports relative to unusual transactions of clients for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations. A document retention policy must include the following: • All necessary records on transactions (both domestic and international) must be maintained for at least five years after the transaction tokes place. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts, currencies, and type of transaction involved) so as to provide, if necessary, evidence for prosecution of criminal behavior. • Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar

		documents), account files and business correspondence must be kept for at least five years after the business relationship has been discontinued. • Administrators and self-administered must ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities. In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure to the FIU/MOT, investigating or law enforcement authority they must be retained until it is confirmed by these parties that the case has been closed.
36.	II.2.A.2. Compliance officer	Each administrator and self-administered investment institution must formally designate one or more senior officer(s) to be responsible for the deterrence and detection money laundering and terrorist financing. The compliance officer must be assigned responsibilities and these must be included in the job description of each designated compliance officer(s). The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.
37.	II.2.A.3. A system of independent testing of policies and procedures	The independent testing must be conducted at least annually by the internal audit department or by an outside independent party such as the external auditor of the administrator or self-administered investment institution. The scope of the testing and the testing results must be documented, with any deficiencies being reported to senior management and/or to the Board of Directors, and to the designated officer(s) with a request for to take corrective actions by a certain deadline.
38.	II.2.A.4. Screening of employees/appropriate training plans and program for personnel	Administrators and self-administered investment institutions must ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are adhered to. Each company must screen their employees on criminal records.

		Administrators and self-administered investment institutions must at a minimum develop training programs and provide training to all personnel who handle transactions susceptible to the activities listed in the National Decree containing general measures and the Ministerial Decree regarding the Indicators for Unusual Transactions. Training must be provided to all new employees dealing with clients, irrespective of their level of seniority. Similarly, training must also be provided to existing members of the staff (such as account and assistant account managers) who are dealing directly with clients. The training must include a clear explanation of all aspects of the laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification and due diligence. For an administrator or self-administered investment institution to be able to demonstrate that it has complied with the aforementioned guidelines with respect to staff training, it must at all times maintain records which include: • details of the content of the training programs provided; • the names of staff who have received the training; • the date on which the training was provided; • the results of any testing carried out to measure staff understanding of the money laundering and terrorist financing requirements; and • an on-going training plan.
39.	II.3 Examination by the Central Bank	All administrators and self-administered investment institutions must be prepared to provide information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the Central Bank before or during an examination and upon the Central Bank's request during the year.

Insurance Companies and Intermediaries (Insurance Brokers)

1.	II.2. Policy statement	Each insurance company's Supervisory Board of Directors and Management must have issued a formal statement of policy which clearly expresses the institution's commitment to combat the abuse of its facilities' financial products and services for the purpose of money laundering and terrorist financing. The policy statement must state the insurance company's intention to comply with current anti-money laundering and terrorist financing legislation and guidelines, in particular the laws and guidelines regarding the identification of customers and the reporting of unusual transactions. The policy statement must cover also the following items:: • The implementation of a formal system of internal control to identify (prospective) clients and deter, detect and report unusual transactions and subsequently keep adequate records of these clients and transactions; • The appointment of one or more compliance officers responsible for ensuring day-to-day compliance with these procedures. The officer(s) must have the authority to investigate unusual transactions extensively; • A system of independent testing of policies and procedures by the insurance company's internal audit personnel, compliance department, or by a competent external source to ensure their effectiveness; • Screening of and preparation of an appropriate training program for personnel to increase employee's awareness and knowledge in the field of money laundering and terrorist financing prevention and detection.
2.	II.2.A. Detection and deterrence of money laundering	Pursuant to the NOIS the life insurance companies and intermediaries must ascertain and record the identity of their customers. Furthermore they must inquire whether or not the party who pays the premium is also the one to whom the distribution will be made.
3.	II.2.A. Foreign branches and subsidiaries	Insurance companies and intermediaries are required to ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with home country requirements and the FATF Recommendations, to the extent that local (i.e., host country) laws and regulations permit. Insurance companies must be required to pay particular attention that this principle is

		observed with respect to their branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations. Where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries are required to apply the higher standard, to the extent that local (i.e., host country) laws and regulations permit. Insurance companies and intermediaries are required to inform the Central Bank when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by local (i.e., host country) laws, regulations, or other measures.
4.	II.2.A. Customer Due Diligence	Insurance companies and their intermediaries have the obligation to determine the true identity of their (prospective) personal and corporate clients/customers, before entering into insurance contracts with them. Insurance companies and intermediaries must develop clear customer acceptance policies and procedures, including a description of the types of customers that are more likely to pose a higher than average risk to the company. The policy must ensure that transactions, must under no circumstance be conducted with customers who fail to provide proof of their identity. Customer due diligence measures that must be taken by insurers include: • identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information; • for all customers, the insurer must determine whether the customer is acting on behalf of another person, and must then take reasonable steps to obtain sufficient identification data to verify the identity of that other person; • identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the insurer is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this must include insurers taking reasonable measures to understand the ownership and control structure of the customer; • obtaining information on the purpose and intended nature of the business relationship; and • conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the insurer's knowledge of the

		customer, their business and risk profile, including, where necessary, the source of funds.
5.	II.2.A. Anonymous customers	Insurers must not offer insurance to customers or for beneficiaries that obviously use fictitious names or are kept anonymous. The latter being the case with so-called bearer policies.
6.	II.2.A. Ongoing Due Diligence	The insurance companies and intermediaries must be required to be alert to the implications of the financial flows and transaction patterns of existing policyholders, particularly where there is a significant, unexpected, and unexplained change in the behavior of the policyholders. The company must be extra vigilant to the particular risks from the practice of buying and selling second hand endowment policies, as well as the use of single premium unit-linked policies. The company must check any reinsurance or retrocession to ensure the monies are paid to bona fide re-insurance entities at rates commensurate with the risks underwritten.
7.	II.2.A. Preventive measures	Insurance companies and intermediaries must take necessary measures in preventing the unlawful use of entities identified as vulnerable, such as charitable or non-profit organizations, to be used as conduits for criminal proceeds or terrorist financing. The required information regarding the customer, the authorized identification documents and the nature of the transaction is legally described and must therefore be adequately documented.
8.	II.2.A. Updated copies of identification document	An important objective for insurance companies and intermediaries is to ensure that documents, data or information collected under the customer due diligence process (know your customer policy) is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships. The requirement on customer due diligence must apply to all new customers as well as –on the basis of materiality and risk- to existing customers. As to the latter the insurer must conduct due diligence at appropriate times.
9.	II.2.A. Identification checklist	The introduction of a checklist for the identification and/or transaction information of customers and a centralized record keeping system must be in place.
10.	II.2.A. Identification resident and non-	The identity of a **resident** and a **non-resident** personal customer must be established through one of the following documents:

	resident customers	• a driver's license; • an identity card; • a travel-document or passport; • any other document to be designated by the Minister of Finance.
11.	II.2.A. Verification of the identity of non-resident customers	Verification of the identity of **non-resident** clients must be obtained by reference to one or more of the following as deemed practical and appropriate: • existing insurance relationships of the prospective customer; • international or home country telephone directory; • personal reference by a known policyholder; • embassy or consulate in home country or address provided by the prospective customer; • in case of personal account check, the check tendered to open the account, comparison of signature thereon; and, • if provided, cross reference address printed on personal check to permanent address provided by client on standard application form. Insurance companies and intermediaries must pay special attention to non resident clients and understand the reasons for which the client has chosen to enter into an insurance contract in the foreign country.
12.	II.2.A. Identification of corporate customers	It is important to identify the nature of the business, account signatures, and the (ultimate) beneficial owner(s). Insurance companies and intermediaries also must obtain personal information on the managing and/or supervisory directors. Copies of the identification documents of all account signatories, including the directors with signing authority on the corporate client's accounts, must be kept on file. The procedures for the identification of personal customers must be applied for the mentioned account signatures' director(s) and all (ultimate) beneficial owners holding a qualifying interest in the company. Insurance companies and intermediaries must ascertain the identity of corporate customers based on reliable identification documents, with preference for originals and official documents attesting to the legal existence, and structure of a company or legal entity. The identity, existence and nature of the corporate customer must be established with the aid of a certified extract from the register of

		the Chamber of Commerce and Industry, or an equivalent institution, in the country of domiciliation. The extract or the identification document must contain at least the information stipulated by the Minister of Finance.
13.	II.2.A. Identification of PEP's	Insurance companies and intermediaries must conduct enhanced due diligence for politically exposed persons (PEPs), their families and associates. The institution's decision to enter into business relationships with PEP's must be taken at its senior management level. The institution must make reasonable efforts to ascertain that the PEP source of wealth and source of funds/ income is not from illegal activities and where appropriate, review the customer's credit and character and the type of transactions the customer would typically conduct. Insurance companies and intermediaries must not accept or maintain a business relationship if the institution knows or must assume that the funds derive from corruption or misuse of public assets. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, financial institutions must obtain senior management approval to continue the business relationship. Where the financial institution is in a business relationship with a PEP, they must conduct enhanced ongoing monitoring on that relationship.
14.	II.2.A. Reliance on intermediaries or other third parties	Insurers must include specific clauses in the contracts with their intermediaries. These clauses must include commitments for the intermediaries to perform the necessary customer due diligence measures, granting access to client files and sending (copies of) files to the insurer upon request without delay. Insurers must inform themselves which jurisdictions are considered suitable to rely on business from intermediaries and third parties. The insurer must undertake and complete its own verification of the customer and beneficial owner if it has any doubts about the third party's ability to undertake appropriate due diligence. If insurers rely on intermediaries or other third parties to perform elements of the CDD process, a service level agreement will be required in case the complete CDD process has been outsourced to an intermediary or third party.
15.	II.2.A. Risk classification	Insurance companies and intermediaries must develop risk profiles for all of its customers to determine which categories of customers expose the institution to higher money laundering and terrorist financing risk. The assessment of the risk exposure and the

		preparation of the risk classification of a customer, must take place after the CDD information mentioned above have been received. The risk profile must comprise of minimally the following possible categories: low, medium and high risk. Insurance companies and intermediaries must apply CDD requirements to existing customers and may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship, or transaction. Insurance companies and intermediaries must at least consider the following risk categories while developing and updating the risk profile of a customer: (i) customer risk, (ii) products/services risk, (iii) country or geographic risk, and (iv) delivery channels risk. The insurance company and intermediary must make its own determination as to the assignment of the risk weights.
16.	II.2.A. Enhanced Due Diligence	Insurance companies and intermediaries must conduct enhanced due diligence in all of the high risk cases/circumstances mentioned under (a) above and in any other cases/circumstances identified by the institution, according to its risk assessment framework. The institution's decision to enter into or to continue business relationships with such customers must be taken at its senior management level. Insurance companies and intermediaries must not accept or maintain a business relationship if the institution knows or must assume that the funds derive from corruption or misuse of public assets, without prejudice to any obligation the institution has under criminal law or other laws or regulations. The insurance company and intermediary must ensure that the identification documents of its high risk categories of customers are at all times valid.
17.	II.2.A. Identification PEP's	Since all PEPs may not be identified initially as such and existing customers may subsequently obtain a PEP status, insurance companies and intermediaries must undertake regular reviews of at least the more important customers to detect if an existing customer may have become a PEP. Additionally, insurance companies and intermediaries are encouraged to conduct enhanced due diligence and continuous monitoring of PEPs who hold prominent public functions domestically.
18.	II.2.A.1. Identification,	Life insurance companies and intermediaries are not only required to adhere to

	verification, and internal control measures for reporting of unusual transactions	the stipulations of the identification regulations, but they are also required to detect and report either proposed or completed unusual transactions. Hence, it is important for every insurance company to have adequate procedures for its personnel in place. These procedures must cover: a) the recognition of unusual transaction; b) the acceptance and documentation of unusual transaction; and c) the reporting of unusual transactions.
19.	II.2.A.1. Recognition of unusual transaction	The insurer must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose for both the establishment of a business relationship and to ongoing due diligence. The background and purpose of such transaction must, as far as possible, be examined; the findings put in writing, and be available to assist competent authorities and auditors. Insurance entities must be alert to the implications of the financial flows and transactions patterns of existing policyholders, particularly where there is significant, unexpected and unexplained change in the behavior of the policyholders' account. All institutions must develop special programs to select objectively defined unusual transactions. Moreover, management must provide its staff with specific guidance and training to recognize and document adequately the unusual transactions based on especially the subjective indicators.
20.	II.2.A.1. Wire transfer	Life insurance companies must be extremely vigilant when premium payments are made or sums are deposited from accounts with banks outside Curaçao and Sint Maarten. If such funds are accepted, suitable identification of the depositor must be obtained. If another party than the policyholder pays, than knowledge about the source of funds must be required through a "Source of Funds Declaration Form".
21.	II.2.A.1. High-risk and non-cooperative jurisdictions	Insurance companies and intermediaries must give special attention, especially in underwriting and claims settlement to business relations and transactions with other financial institutions, including intermediaries and individuals, companies and other corporate vehicles, from the high-risk and non-cooperative jurisdictions. If insurance companies and intermediaries find that such a transaction is unusual, this must be reported to the FIU/MOT.

22.	II.2.A.1. Policies and procedures non-face-to-face customers	The insurers need to have policies and procedures in place to address the specific risks associated with non face-to-face business relationships or transactions.
23.	II.2.A.1. Misuse of technological development	Insurance companies and intermediaries are required to have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.
24.	II.2.A.1. Documentation of unusual transactions	To guard against money laundering and terrorist financing, it is important for insurance companies and intermediaries to provide an audit trail for suspicious funds.
25.	II.2.A.1 Reporting of unusual transactions	Insurance companies and intermediaries must have clear procedures which are communicated to their personnel for the reporting of unusual transactions. The obligation to report internally, without delay, lies on anyone who renders financial services by virtue of his profession or in the ordinary course of his business. All transactions as mentioned in the list of indicators of the NORUT, must be referred to the designated officer(s), in a format which contains at least the data as stipulated by law. The designated officer(s) must keep an adequate filing system for these records. If internally reported transactions are not reported to the FIU/MOT by the institution, the reasons therefore must be adequately documented and signed off by this officer and/or by management. A report must be prepared of all unusual transactions by the designated officer(s) for external reporting purposes. The report must be submitted to management for their review for compliance with existing regulations, and their authorization for submission to the FIU/MOT. Copies of these reports must be kept by the reporting institution. If an unusual transaction is not authorized by management to incorporate in the report to the FIU/MOT, all documents relevant to the transaction including the reasons for non-authorization must be adequately documented, signed off by the designated officer and management and kept by the reporting institution. Management must establish a policy to ensure that:

		- the insurance company and its Supervisory Board of Directors, management and employees do not warn customers when information about them is being reported to the FIU/MOT, or on internal inquiries being made by the institution's compliance staff on them; - the insurance company and its Supervisory Board of Directors, management and employees follow the instructions from the FIU/MOT to the extent that they carry out further investigation or review. The same holds for inquiries made by either the justice department or the public prosecutor.
26.	II.2.B. Detection and deterrence of terrorist financing	Insurance companies and intermediaries must take into account the characteristics including types of transactions listed in the annex 1 to the FATF document "Guidance for Financial Institutions in Detecting terrorist Financing. Those characteristics and transactions could be a reason for additional scrutiny and could indicate funds involved in terrorist financing. In addition, insurance companies and intermediaries must take into account other available information, including any (updated) lists of suspected terrorists, terrorist groups, and associated individuals and entities. Insurance companies and intermediaries must verify whether a client's name appears on above-mentioned lists. If a insurance company and intermediary encounters a match they must freeze the asset of the client and inform the Central Bank immediately. In addition, insurance companies and intermediaries must be vigilant in the abuse of non-profit organizations for terrorist financing. The institutions must observe the FATF's Special Recommendation (SR) VIII. If an insurance company or an intermediary suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or by terrorist organizations, it must report promptly its suspicion to the FIU/MOT.
27.	II.2.B. Record keeping	Insurance companies and intermediaries must ensure compliance with the record keeping requirements contained in the relevant money laundering and terrorist financing legislation. The investigating authorities need to ensure a satisfactory audit trail for suspected transactions related to money laundering and terrorist financing and be able to establish a financial profile of the suspect

		policyholder. Where appropriate, insurance companies and intermediaries must consider retaining certain records e.g. customer identification and business correspondence, and internal and external reports relative to unusual transactions of clients, for periods which may exceed that required under the relevant money laundering and terrorist financing legislation, rules and regulations. A document retention policy must include the following: • All necessary records on transactions, both domestic and international, must be maintained for at least five years. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts, currencies, and type of transaction involved) so as to provide, if necessary, evidence for prosecution of criminal behavior. • Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence must be kept for at least five years after the account is closed. • Insurance companies and intermediaries must ensure that all customer and transaction records and information are available on a timely basis to the domestic competent authorities. In situations where the records relate to on-going investigations or transactions which have been the subject of disclosure to the MOT, investigating or law enforcement authority they must be retained until it is confirmed by these parties that the case has been closed.
28.	II.2.A.2. Compliance officer	Each insurance company must formally designate one or more senior officer(s) to be responsible for the deterrence and detection money laundering and terrorist financing. The compliance officer(s) must be able to act independently. The compliance officer must be assigned responsibilities and these must be included in the job description of each designated officer. The job description must be signed off and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.
29.	II.2.A.3.	Independent testing of the adequate functioning of the policies and

	A system of independent testing of policies and procedures	procedures must be conducted at least annually by an adequately resourced internal audit department or by an outside independent party such as the institution's external auditors. The scope of the testing and the testing results must be documented, with any deficiencies being reported to senior management and/or the Supervisory Board of Directors, and to the designated officer(s) with a request to take corrective actions by a certain deadline.
30.	II.2.A.4. Screening of employees/appropriate training plans and program for personnel	Insurance companies and intermediaries must ensure that their business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are adhered to. Each company must establish and adhere to proper policies and procedures to screen their employees on criminal records. Insurance companies and intermediaries must at a minimum develop training programs and provide training to all personnel who handle transactions susceptible to the activities listed in the National Decree containing general measures and the Ministerial Decree regarding the Indicators for Unusual Transactions. As far as new employees are concerned, training must be provided to all new employees dealing with customers, irrespective of their level of seniority. Similarly, training must also be provided to existing members of the staff who are dealing directly with the public such as cashiers and agents. The training must include a clear explanation of all aspects of the existing laws or executive decrees relating to money laundering and terrorist financing and requirements concerning customer identification and due diligence. In order for an insurance company to be able to demonstrate that it has complied with the aforementioned guidelines with respect to staff training, it must at all times maintain records which include: • details of the content of the training programs provided; • the names of staff who have received the training; • the date on which the training was provided; • the results of any testing carried out to measure staff understanding of the money laundering and terrorist financing requirements; and • an on-going training plan.

31.	II.3 Examination by the Central Bank	All insurance companies and intermediaries must be prepared to provide information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the Central Bank before or during an on-site examination and upon the Central Bank's request during the year.

Please note that this list of compulsory requirements is subject to change.

Appendix II

The legal provisions of the supervisory legislations:

- The National Ordinance on the Supervision of Banking and Credit Institutions (N.G. 1994, no 4) (NOSBCI), article 21, paragraph 2, section e for credit institutions;
- The National Ordinance on the Supervision of Investment Institutions and Administrators (N.G. 2002, no. 137) (NOSIIA), article 9 paragraph 1, and article 18, paragraph 1 for, respectively, investment institutions and administrators;
- Regulations for Foreign Exchange Transactions Curaçao and Sint Maarten (NG. 2010, no. 112[1]) (RFETCSM), article 21, paragraph 1 for money transfer companies;
- The National Ordinance on the Supervision of Trust Service Providers, (N.G. 2003, no 114) (NOSTSP) article 11, paragraph 1 for company service providers[2].

[1] N.G.: National Gazette, official national publication: "publicatieblad" of "afkondigingsblad" in Dutch
[2] The activities of trust service providers operating in the Curaçao and Sint Maarten are similar to those of company service providers operating in other jurisdictions.