Good practice Wwft BES

Manual

DeNederlandscheBank

EUROSYSTEEM

Content

DNB Good Practices disclaimer – purpose and coherence of the legal framework

The Anti-Money Laundering and Anti-Terrorist Financing (BES) Act *(Wet ter voorkoming van witwassen en financieren van terrorisme BES – Wwft BES)* includes the provisions that service providers in the Caribbean Netherlands must comply with in their operational management to counter money laundering and terrorist financing. This Good Practices document has been drawn up to assist service providers in complying with these requirements. However, service providers at all times bear full responsibility for compliance with the relevant legal provisions.

This Good Practices document provides a schematic illustration of elements of the *Wwft BES* and recommendations for service providers on compliance with the Anti-Money Laundering and Anti-Terrorist Financing Act in the Caribbean Netherlands. In the document we (De Nederlandsche Bank N.V. – DNB) set out our views, based on our observations and expectations, on the practices through which policy is implemented. We consider that these practices must include proper application of the rules to which this Good Practices document relates.

Our intention with this document is to encourage service providers to consider its provisions, without being obliged to do so, while also taking their own specific circumstances into account. The document illustrates the conduct we have observed or expect to see in policy practice. It is only indicative, so some service providers may need to apply the underlying regulations differently and possibly more strictly. Service providers can exercise discretion in their application of the best practices, but they bear full responsibility for compliance with the *Wwft BES*.

The Good Practices document uses terms defined in Section 1 of the *Wwft BES*. It may also use terms that differ from these definitions or other provisions. In case of doubt the legal texts will prevail.

Introduction

This Good Practices document schematically explains three core processes in the *Wwft BES*: customer acceptance, customer and transaction monitoring and customer review. At present, the document is limited to explaining these and a number of other obligations in the *Wwft BES*. It may be expanded at a later stage to cover other elements of the *Wwft BES*, including those relating to trust offices. This document does not replace the *Wwft BES* but is intended to assist BES service providers with its application. The provisions of the *Wwft BES* that are not covered in this document nevertheless continue to apply in full.

The Good Practices document is structured as a guide for BES service providers that are supervised by DNB under the *Wwft BES*. The main text is a factual presentation of the *Wwft BES* without any interpretation on our part. The accompanying square text boxes contain descriptions of good practices. These may be interpretations of the way in which we believe certain provisions can be fulfilled, supported by examples, or an indication of what we expect to find when supervising an institution's compliance with the *Wwft BES*.

This Good Practices document is applicable to all service providers falling within the scope of the *Wwft BES* and under the supervision of DNB. It does not yet cover the elements relating specifically to trust offices.

1. Governance and general matters

This Good Practices document provides guidance on the organisation of core processes for the prevention of money laundering and terrorist financing, for which the *Wwft BES* specifies various organisational parameters.

1.1 Risk analysis (Section 1.9 of the *Wwft BES*)

A service provider must take measures to identify and assess its risks of money laundering and terrorist financing, such measures being in proportion to the nature and size of the service provider. In analysing the risk, the service provider must take into account the risk factors associated with the types of customers, products, services, transactions and supply channels, as well as countries or geographies. The service provider must also take into account the risks included in the national risk assessment (NRA BES), which forms part of the systematic integrity risk analysis (SIRA).

The risk analysis must be updated periodically and in response to the latest events. The current risk analysis has been documented and forms the basis for the required control measures (rules of conduct, procedures and measures).

1.2 Internal organisation (Section 1.10 of the *Wwft BES*)

Service providers have a set of written rules of conduct, procedures and measures that set out in factual terms how they mitigate risks of money laundering and terrorist financing and the specific risks included in the national risk assessment (NRA BES). In any event, the rules of conduct, procedures and measures describe the three main processes set out in this Good Practices document.

Service providers must ensure that these rules of conduct, procedures and measures are regularly evaluated and updated. This is the responsibility of the policymaker designated by the service provider.[1]

The rules of conduct, procedures and measures are proportionate to the nature and size of the service provider. This means that a service provider exposed to high risks must have a more detailed and in-depth description than one exposed to relatively low risks.

1.3 Governance (Section 1.11 of the *Wwft BES*)

If two or more persons are responsible for the service provider's day-to-day policy, one of them is assigned responsibility for compliance with the provisions of the *Wwft BES*, and hence also for the proper implementation of the processes described in this Good Practices document (the '*Wwft BES* policymaker').

1.4 Compliance and audit

A service provider must also have an independent and effective compliance function, to the extent appropriate to its nature and size. The compliance function must be focused on monitoring compliance with the *Wwft BES* and the service provider's internal rules.

A service provider must have an independent audit function, to the extent appropriate to its nature and size. The independent audit function monitors a service provider's compliance with the *Wwft BES* and the performance of the compliance function.

It is important that the management, and particularly the '*Wwft BES* policymaker', ensures that these functions are organised effectively and proportionately.

1 Section 1.1 of the *Wwft BES*.

Good practices in the compliance function

The key points with regard to the performance of the compliance function are as follows:

- The position of the compliance function is laid down in a compliance charter.
- The compliance charter states that the compliance function has access to all information, premises and personnel. It also states to whom the compliance function reports and stipulates that the compliance function has direct access to the supervisory board.
- The compliance function must have the necessary professionalism, authority, capacity and resources and can independently engage expertise if necessary.
- The duties of the compliance function are set out in a compliance programme, which is determined independently by the Head of Compliance.
- The compliance function has sufficient scope to monitor compliance with the *Wwft BES* and to examine customer files and transactions.
- Reports on compliance with the *Wwft BES* are sent to the '*Wwft BES* policymaker' periodically, for example each quarter.
- Any deficiencies identified must be resolved by the management under the supervision of the compliance function.
- The compliance programme includes periodic updates of the integrity risk analysis.

Good practices in the audit function

The key points with regard to the performance of the audit function are as follows:

- The audit function operates independently.
- The audit function verifies compliance with the *Wwft BES* and the performance of the compliance function at least once a year.
- The audit function records the findings in a report.
- The service provider then refines the measures on the basis of the findings.

1.5 Proportionality

Proportionality in the above matters is maintained with the close involvement of any policymakers and group functions/parent companies.

2 Customer acceptance

Click here to access flowchart

2.1 Business relationship or relevant one-off transaction?

Customer due diligence is conducted in the following cases:[2]

- Upon entry into a business relationship, defined as a professional or commercial relationship between a service provider and a natural person or legal entity that is related to the service provider's professional activities and is expected to continue for a certain period from the time the relationship is entered into.[3]
- Where there is no business relationship, in the case of a one-off transaction:[4]
  - payment of a life insurance benefit ≥ USD 11,000[5]
  - transaction involving vehicles, precious stones, precious metals, jewellery or gems, or intermediation in such transactions ≥ *USD 11,000[6]
  - transaction associated with the operation of games of chance, including gaming casinos ≥ USD 3,000[7]
  - transaction ≥ USD 0 associated with services other than the three referred to above.[8]

A service provider must demonstrably adapt the customer due diligence to the sensitivity to the risk of money laundering or terrorist financing pertaining to the type of customer, business relationship, product or transaction.[9]

Good practice: demonstrable adaptation of customer due diligence

- Service providers must conduct and document a policy that takes account of the risks associated with the type of customer and service.
- The risks associated with a customer are assessed in accordance with the service provider's policy and the assessment is entered in the customer file.
- The information used by the service provider in the customer due diligence is recorded in a single customer file.
- The service provider guarantees compliance with the law and the service provider's internal rules: the compliance function verifies that the customer due diligence has been demonstrably adapted to the sensitivity to the risk of money laundering or terrorist financing pertaining to the type of customer, business relationship, product or transaction.

2 Section 2.3(1) of the *Wwft BES.*.
3 Section 2.3(1)(a) in conjunction with Section 1.1(1)(v) of the *Wwft BES.*
4 Explanatory Memorandum to the *Wwft BES.*, p. 11.
5 Section 2.3(1)(b) of the *Wwft BES.* in conjunction with Section 2 of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation in conjunction with Annex A(I)(f) of the *Wwft BES.*.
6 Section 2.3(1)(b) of the *Wwft BES.* in conjunction with Section 2 of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation in conjunction with Annex A(I)(m) of the *Wwft BES.*.
7 Section 2.3(1)(b) of the *Wwft BES.* in conjunction with Section 2 of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation in conjunction with Annex A(I)(j) of the *Wwft BES.*.
8 Section 2.3(1)(b) of the *Wwft BES.* in conjunction with Section 2 of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
9 Section 2.2(3) of the *Wwft BES.*.

2.2 No business relationship or transaction without customer due diligence

Customer due diligence is conducted before the service provider enters into a business relationship or executes a one-off transaction.[10]

There are a number of exceptions:

- The service provider is permitted to verify the identity of the customer and the UBO during the process of entering into the business relationship, provided this is necessary to avoid disrupting the service and provided the risk of money laundering or terrorist financing is low. In such cases the service provider must verify the identity as soon as possible after the initial contact with the customer.[11]
- A life insurer is permitted to identify the beneficiary of a policy and to verify the identity after the start of the business relationship. In that case the identification and verification of identity must take place at or before the time of payout, or at or before the time at which the beneficiary wishes to exercise their rights under the policy.[12]
- A credit service provider is permitted to open an account before the customer's identity has been verified, provided it ensures that the account cannot be used until the identity has been verified.[13]

2.3 Introduced customer

Prior customer due diligence is not required in the case of a customer introduced to a service provider by a 'designated service provider' that has already carried out the identification and verification:[14]

- a lawyer, civil law notary or junior civil law notary established in the BES Islands;
- an investment service provider, life insurer, life insurance broker, credit service provider or money transaction office licensed under the Financial Markets (BES) Act (*Wet financiële markten BES – Wfm BES*).

Introduction concerns the following cases:[15]

- where a designated service provider acts for a customer;
- where a designated service provider introduces a customer.

At the time of introduction the accepting service provider must have the customer's and the UBO's identification and verification details that the designated service provider used in the customer due diligence.[16] The accepting service provider may also have the relevant data that led to the acceptance of the customer. The accepting service provider is also responsible for drawing up the risk profile and requires the correct information for that purpose.

10 Section 2.4(1) and (2) of the *Wwft BES*.
11 Section 2.7(1) of the *Wwft BES*.
12 Section 2.7(2) of the *Wwft BES*.
13 Section 2.7(3) of the *Wwft BES*.
14 Section 2.6 of the *Wwft BES*.
15 Explanatory Memorandum to the *Wwft BES*, p. 11.
16 Section 2.6(b) of the *Wwft BES*.

If the designated service provider cannot provide the information, the accepting service provider will conduct the customer due diligence required pursuant to the *Wwft BES* or the internal rules.

2.4 Low risk and simplified customer due diligence

A service provider must assess whether there is a low risk of money laundering or terrorist financing. It must demonstrably gather sufficient information to determine whether a business relationship, transaction or customer by its nature poses a low risk.[17]

In their risk assessment service providers must take account of the list of (non-exhaustive) risk factors referred to in the *Wwft BES* and the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation (see below). These factors guide service providers in their assessment of whether a situation entails low risk. The stated examples are not exhaustive, however. Service providers must draw up policy and procedures on the basis of their risk assessment and identify the cases in which there is low risk.

Factors indicating low risk are:[18]

- Customer risk factors:
  - companies listed on exchanges with adequate transparency concerning UBOs;
  - public authorities or government-owned enterprises;
  - customers resident in lower-risk geographic regions (see below).
- Product, service, transaction or delivery channel risk factors:
  - life insurance policies with low premiums;
  - insurance policies for pension schemes which have no early surrender option and cannot be used as collateral;
  - a pension, superannuation or similar scheme that provides retirement benefits for employees, where contributions are made by way of deductions from pay and the scheme rules do not permit the assignment of a member's rights under the scheme;
  - financial products or services that provide defined and limited services, so as to increase access for financial inclusion purposes;
  - products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership.

17 Section 2.8(2) of the *Wwft BES*.
18 Section 2.8 of the *Wwft BES* in conjunction with Section 7(2) and Annex C of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.

- Geographic risk factors — registration, establishment or residence in:
  - countries having effective AML/CFT systems;
  - countries identified by credible sources as having a low level of corruption or other criminal activity;
  - countries identified by credible sources such as mutual assessments, detailed evaluation reports or published follow-up reports as having rules in place to combat money laundering and terrorist financing that are consistent with the revised FATF Recommendations and effectively implement those rules.

Low risk certainly applies in the following cases:[19]

- life insurance policies with an annual premium ≤ $1,000 or a single premium ≤ $2,500;
- life insurance in which the first premium payment is debited from or the benefit payment is credited to an account belonging to the customer with a credit service provider or a life insurer licensed under the *Wfm BES*;
- Pension products as referred to in Section 1 of the BES Pensions Act (*Pensioenwet BES*);
- Deposit, opening or effecting of a payment, in connection with securities trading, by an institution licensed as a credit institution under the *Wfm BES* or in a country designated by the Minister.

Simplified customer due diligence applies to the following customer categories[20]:

- financial undertakings licensed under the *Wfm BES*,
- government agencies of the public bodies or the European part of the Netherlands, and
- companies listed on an exchange in a designated country.

Simplified customer due diligence

If a business relationship, transaction or customer by its nature poses a low risk of money laundering or terrorist financing, the service provider may conduct simplified customer due diligence.[21]

The conclusion that simplified customer due diligence is appropriate is always based on a risk assessment. A risk assessment will be carried out in all cases, after which the intensity of the customer due diligence will be adapted to the estimated risk. The service provider may carry out a prior assessment of the cases in which simplified customer due diligence will be conducted. This will involve a prior risk analysis taking into account the risk factors that identify low-risk customers. The service provider documents this in the policy.

19 Section 2.8 of the *Wwft BES* in conjunction with Section 4(1) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Decree.
20 Section 2.8 of the *Wwft BES* in conjunction with Section 4(2) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Decree
21 Section 2.8(1) of the *Wwft BES*.

The law does not specify the content of simplified customer due diligence. For customers on whom simplified customer due diligence has been conducted a service provider will have sufficient data to fulfil its obligation to report unusual transactions.[22] Simplified customer due diligence will logically include:

- identification of the customer and verification of identity
- identification of the UBO
- establishing whether the natural person representing the customer has the authority to do so, and identifying this person
- determining the risk category (in the case of simplified customer due diligence this must always be low, of course)

In the case of a business relationship (i.e. not a one-off transaction), the service provider must draw up a risk profile/transaction profile (see below).[23]

Wire Transfer Regulation (WTR)

Credit institutions, money transaction offices and electronic money institutions provide the following information on the payer and the payee in the case of money transfers:[24]

- full name
- address or place and date of birth of the payer or their customer identification number
- account number (if the payer's account number is not known, it is replaced by a unique identification code enabling the money transfer to be traced back to the payer).

Credit institutions, money transaction offices and electronic money institutions must check whether received payments include the correct payer information. If the information has not been transmitted, they will refuse the payment. If payments originating from the same payment service provider often lack the correct information, termination of the relationship with that payment service provider may be considered. In such cases the service provider will also consider whether to file an unusual transaction report.[25]

22 Section 2.8(4) in conjunction with Section 3.5(2) of the *Wwft BES*.
23 Section 2.5(1) of the *Wwft BES*.
24 Section 4.19 of the *Wfm BES* in conjunction with Section 3.5 of the Financial Markets (BES) Regulation 2012 (*Regeling financiële markten BES – Rfm BES*). See also the Explanatory Memorandum to the Financial Markets (BES) Regulation 2012, pp. 27 ff.
25 Explanatory Memorandum to the Financial Markets (BES) Regulation 2012, p. 28.

2.5 Regular customer due diligence

The customer due diligence consists of the following elements:

2.5.1 Identifying customers and verifying their identity[26]

A natural person's identity is verified using documents, data or information from reliable and independent sources.[27] These are:[28]

- a driving licence valid in the issuing country
- an identity card valid in the issuing country
- a travel document or passport valid in the issuing country
- the original of a valid residence permit, accompanied by a valid passport
- a copy of a valid residence permit, accompanied by a copy of a valid passport and a declaration by the competent authorities.

Good practice

In some cases a service provider takes measures that go beyond what may be expected in terms of effective risk control. An example is requesting a valid ID from the customer if the ID in the customer file – which was valid when the identity was verified – has expired. That is not necessary, since the file shows that the customer's identity was verified before acceptance.

The identity of a legal entity established in the BES Islands is verified using documents, data or information from reliable and independent sources.[29] These are:[30]

- a certified extract from the trade register of the Chamber of Commerce
- a deed or declaration drawn up or issued by a lawyer, public law notary or junior public law notary established in the public bodies.

26 Section 2.2(2)(a). of the *Wwft BES*.
27 Section 2.12(1) of the *Wwft BES*.
28 Section 2.12(1) of the *Wwft BES* in conjunction with Section 4(1) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
29 Section 2.12(1) of the *Wwft BES*.
30 Section 2.12(1) of the *Wwft BES* in conjunction with Section 4(2) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.

The identity of a foreign legal entity is verified on the basis of reliable and internationally accepted documents, data or information or on the basis of documents, data or information recognised as a valid means of identification by the law of the customer's country or state of origin.[31] These are:[32]

a. a certified extract from the register of service providers comparable to the Chamber of Commerce, including:[33]
   i. for the legal entity: the legal form, registered name, trade name, full address, registered office address, country of registered office and, if the legal entity is registered with a Chamber of Commerce and Industry or similar body, the registration number and the country or island territory in which such Chamber or similar body is established;
   ii. for all authorised agents and representatives: the name, date of birth and document used for identification.
b. a declaration issued by an official from the country of establishment who is independent of the customer and can, by virtue of their position, sufficiently guarantee the reliability of this declaration, which must include the same information as in (i).

2.5.2 Identification of the UBO and verification of their identity, supported by information on the customer's ownership and control structure[34]

The customer due diligence includes the determination by the service provider of the identity of the ultimate beneficial owner (UBO) (identification and verification). The service provider must therefore identify the UBO(s) in respect of each customer. A UBO is always a natural person. This rule applies not only when the customer is a legal entity, such as a legal person or foundation, or a legal structure, such as a trust, but also when the customer is a natural person over whom another natural person has effective control or for whose account a transaction or activity is conducted.

Who is considered to be the UBO?[35]

The law states that a person or ultimate owner qualifies as the UBO of a legal entity, for example, in the following three cases:

1. If the person has direct or indirect formal control of more than 25%.
2. If the person can exercise effective control.
3. If the person is a 'pseudo-UBO'. In this case the members of the senior management are considered to be the UBO if none of the UBOs referred

31 Section 2.12(2) of the *Wwft BES*.
32 Section 2.12(1) of the *Wwft BES* in conjunction with Section 4(3) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
33 Section 2.12(1) of the *Wwft BES* in conjunction with Section 4(4) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
34 Section 2.2(2)(b) of the *Wwft BES*.
35 Section 2 of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Decree.

to in 1 or 2 have been discovered after all possible means have been exhausted and on condition that there are no grounds for suspicion. Hence this is a fallback option.[36]

The requirement to identify the UBOs can usually be fulfilled by having the customer declare who the UBO is. The service provider must then take reasonable steps to verify the declared identity, as the veracity of the information provided by the customer has not yet been verified. The verification involves a risk assessment based on independent and reliable sources, such as public sources, an extract from the trade register or confirmation of the party's declaration by an independent third party.

A service provider must always verify the identity of the UBO, regardless of the risk level. The identity must therefore always be verified, but the method and depth of the verification is risk-based. This means that more extensive measures are taken in the case of high-risk customers than low-risk customers. The verification measures provide the service provider with sufficient information to convince itself of the identity of the UBO. In all cases the service provider must also check whether the UBO is a PEP (politically exposed person).

Good practice

A bank's customer has an extensive, multi-layered structure. Some of its shareholders are based in high-risk jurisdictions. In view of the risks identified in this customer relationship, the bank does not believe UBO self-certification is sufficient. The bank uses information from independent and reliable sources (such as extracts from trade registers) to map the ownership structure and identifies three individuals who each have indirect formal control in excess of 25%. The service provider documents the results (i.e. the sources, analysis and conclusions) of the investigation in the customer file.

Such documentation is an essential part of the UBO customer due diligence procedure. It goes without saying that a service provider must record the measures taken to identify the natural person who is the UBO and, if applicable, the reason for designating one or more members of the senior management as the UBO.

36 According to Section 2(6) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Decree senior management comprises exclusively: each director within the meaning of Section 14 of Book 2 of the BES Islands Civil Code, or, in the case of a partnership, each partner, with the exception of a sleeping partner as referred to in Section 15 of the BES Islands Commercial Code.

Information on the customer's ownership and control structure

The service provider must also have adequate risk-based measures in place to understand the customer's ownership and control structure in the case of legal entities, foundations, trusts and other legal structures. These include measures to verify the legal status of customers other than natural persons, if possible by obtaining proof of incorporation.

The guiding principle is that the service provider must know and understand this structure. To this end the service provider also examines the customer's reasons for using complex structures. This can be done by making enquiries of the customer, but also, for example, by requesting a legal or tax opinion or advice.

Good practice

A legal entity that wishes to become a customer is part of a larger structure. The parent company is established on another Caribbean island and there are subsidiaries in Montenegro, Cyprus, Nevis and Anguilla, amongst others. The prospective customer holds the image rights of a number of footballers.

The service provider asks about the reason for the structure. The representative of the legal entity responds by presenting tax advice issued by a Big Four accounting firm to explain the structure. However, the service provider still does not properly understand the prospective customer's role in the structure and therefore considers the risk too high. When questioned, the customer is still unable to provide sufficient clarity. The customer is refused.

2.5.3 Representation[37]

During the customer due diligence the service provider must determine whether the natural person representing the customer is authorised to do so. Where appropriate, the service provider must identify the natural person and verify their identity. This applies for example in a situation in which a natural person acts as a legal entity's director.

37 Section 2.2(2)(e) of the *Wwft BES*.

If a natural person acts on behalf of a legal entity which, in turn, is a director of another legal entity, the chain of representative powers must be established.[38] An extract from the Trade Register of the Chamber of Commerce may for example be used for this purpose.

2.5.4 Verifying whether the customer is acting on their own behalf or for a third party[39]

During the customer due diligence process the service provider must establish whether the customer is acting on their own behalf or for another party. This obligation refers to the practice of using persons who act in their own name but are actually acting on behalf of third parties and possibly criminals.[40]

Service providers can concentrate their efforts on cases that appear to pose a higher risk, in other words applying a risk-based approach. The service provider must take reasonable steps to ascertain whether a person is acting on their own behalf or for another party. To this end a service provider can define indicators, for example, to be used in the customer due diligence.

These may include instances where the person is unable to answer certain questions, for example about the source of the funds, or where unclear, vague reasons are given for the transaction.

If the service provider suspects that the customer is not acting on their own behalf, this naturally represents a higher or unacceptable risk. If it is clear that a customer is acting for someone else, that third party qualifies as the customer, so the customer due diligence obligations also apply with regard to that person.

2.6 Politically exposed persons (PEPs)

A service provider must ensure that procedures are in place to determine whether the customer (including UBOs) is a PEP.[41]

A PEP is a politically exposed person. The following qualify as PEPs:[42]

- a person who is or has been entrusted with a prominent public function in or outside the public bodies,
- immediate family members or close associates of that person.
  - Immediate family members are the spouse/partner, partner equivalent to a spouse, children and their spouses/partners, parents.[43]

38 *Parliamentary Papers II* 2011/12, 33 238, no. 3, p. 13.
39 Section 2.2(2)(f) of the *Wwft BES*. See also *Parliamentary Papers II* 2011/12, 33 238, no. 3, p. 4.
40 *Parliamentary Papers II* 2011/12, 33 238, no. 3, p. 13.
41 Section 2.10(3) of the *Wwft BES*.
42 Section 1.1(1)(o) of the *Wwft BES*
43 Section 1.2(1) of the *Wwft BES*.

- Close associates are:[44]
  - a natural person who is known to be the joint UBO of legal entities or legal structures with a PEP or to have other close business relations with that person;
  - a natural person who has sole beneficial ownership of a legal entity or legal structure which is known to have been set up for the benefit de facto of a PEP.

The PEP definition enables service providers to assess independently whether individuals are PEPs. At any rate they are individuals holding senior positions in the government, supreme courts of law, parliament, the army and the diplomatic corps. In addition, individuals may qualify as PEPs when they are entrusted with a public function, but also when it is well known that they exercise political influence because of their administrative, managerial or supervisory position in a political party, a state-owned public limited liability company or a foundation. It is the responsibility of the service provider to determine whether a person qualifies as a PEP.[45]

A person who has terminated their prominent public function at least a year earlier is no longer considered to be a PEP.[46]

Additional measures in the case of a PEP

The provision of services for PEPs requires additional measures because it entails higher integrity and reputational risks. In the case of a PEP the following additional measures apply in any event (including in the case of pseudo-UBOs qualifying as PEPs):[47]

- the decision to enter into the relationship or execute the transaction must be taken or approved by persons who have been authorised to do so by the service provider,[48]
- adequate measures must be in place to ascertain the origin of the assets used in the business relationship or transaction,
- the business relationship must be constantly monitored.

Service providers that have PEPs as customers may set up their internal procedures for constant monitoring of the business relationship in a risk-based manner. For example, children of a Member of Parliament in the Netherlands with a simple payment account may be less risk-sensitive than

44 Section 1.2(2) of the *Wwft BES*.
45 *Parliamentary Papers II* 2019/20, 35 458, no. 3, p. 21.
46 Section 1.1(1)(o) of the *Wwft BES*
47 Section 2.10(3) of the *Wwft BES*.
48 Such approval must be granted by a person with sufficient knowledge of the service provider's exposure to money laundering and terrorist financing risks and sufficient seniority to take decisions affecting its risk exposure (Article 3(12) of Directive (EU) 2015/849).

the spouse of a head of state of a country with a higher corruption risk who opens a private banking account. Nevertheless, PEPs essentially represent higher risk. It may be useful in this regard to be aware of the level of corruption in the country in which the individual has been entrusted with the function. for example by referring to the Corruption Perception Index from Transparency International.

If the customer or a UBO becomes or is found to be a PEP during the business relationship, the service provider must take these additional measures as quickly as possible. Establishing the source of wealth of a UBO who is a PEP can be particularly difficult in some situations, although the intensity of the investigative efforts can be geared to the risk. In cases where it proves impossible to establish the source of the wealth, the service provider can demonstrate that it has made sufficient efforts to discover the source.

Good practice – How should service providers deal with PEPs?

- When entering into a business relationship or executing a transaction, service providers should check whether the customer, or the UBO of the customer, is a PEP.
- This check is repeated periodically, and in the event of alerts or changes.
- The PEP is part of the risk assessment or forms a separate risk category. If PEPs are not accepted, this is deemed to constitute a risk category: unacceptable risk.
- Decisions on the acceptance of PEPs are taken by the senior management.
- The compliance function is involved in decision-making, signing off or in an advisory role in cases involving a PEP.

2.7 Purpose and nature of the business relationship

In the case of business relationships the purpose and intended nature of the relationship must be determined.[49] A service provider can thus estimate any risks arising from the provision of the service for a customer. Some of the required information will usually emerge during contact prior to the business relationship. The purpose of the relationship will also be apparent from the services or products purchased by the customer.[50]

49 Section 2.2(2)(c) of the *Wwft BES*.
50 *Parliamentary Papers II* 2007/08, 31 238, no. 3, p. 18.

In the case of customers not established in the BES Islands, a service provider must clearly understand why the customer is purchasing services or products in the BES Islands. The service provider must assess the acceptability of the stated reasons.

It is important to determine the purpose and intended nature of the business relationship at an individual level before it begins.[51]

2.8 Source of funds

Customer due diligence requires a service provider to investigate the source of the funds used in a business relationship or transaction if necessary. The service provider must include statements and objective and independent documentary evidence of the source of funds in the customer file and make additional enquiries where necessary. The fact that the funds originate from a regulated service provider does not exempt the service provider from performing an independent due diligence review.

To assess the plausibility that the funds originate from a legal source, the service provider must identify specific indicators that determine the depth of the investigation. Possible combinations of indicators are the amount involved, the stated explanation for the origin of the funds, the customer's age and occupation or business activities, the country of origin or destination of the funds and the product or service supplied. In the case of life insurance, the indicators could be, for example, the amount of the initial premium or any additional premiums. Specifically in the case of high risk, it is appropriate to assess the plausibility of the origin of the funds using independent and reliable sources and to record it in the customer file. This also applies to private banking customers.

In order to verify the source of the funds used in the business relationship, it may also be necessary to understand the customer's financial position, especially in the case of high-risk customers. In the case of customers who spread their assets, the service provider must also be aware of assets held elsewhere in order to draw up a correct risk profile. The service provider is responsible for documenting its review of the origin of funds.

51 Rotterdam Court of Law, 5 February 2021.

2.9 Risk profile/transaction profile

A risk profile must be drawn up for each business relationship.[52]

Factors that service providers must take into account as a minimum:[53]

1. the purpose of an account or relationship
2. the size of the assets deposited by a customer or the size of the transactions effected
3. the regularity or duration of the business relationship.

This enables service providers to compare transactions against the customer's risk profile. To determine a customer's risk profile, service providers prepare a transaction profile based on the expected transactions or the expected use of the customer's (or customer group's) account. In this way service providers can monitor transactions effected during the relationship to ensure that they are consistent with their knowledge of the customer and the associated risk profile.

2.10 Higher risk and enhanced customer due diligence

In addition to the regular customer due diligence, a service provider must conduct more detailed due diligence if there is a higher risk of money laundering or terrorist financing.[54]

2.10.1 Enhanced customer due diligence

In cases where the service provider believes there is a higher risk of money laundering or terrorist financing, the service provider must take additional measures (on top of the regular measures). These measures vary according to risk. The additional measures depend on the service provider's risk assessment with regard to the customer, transaction, product and country or region concerned.

When accepting customers purchasing a product with an enhanced risk, for example products or combinations of products which deviate from standard products, standard procedures are not sufficient. The service provider must therefore do more than merely check whether the customer or other stakeholders appear on the sanction lists, whether they are creditworthy or whether their identity documents are genuine, and whether the customer appears in service providers' internal or external warning systems.

Such additional information may relate to the reputation of the customer or the UBO, but also the reputation of persons with whom they are associated. This includes the acquisition and assessment of information on business activities and background information on the customer. As part of enhanced customer due diligence, the service provider must also conduct a deeper investigation into the source of the funds.

52 Section 2.5(1) of the *Wwft BES*.
53 Section 2.5(2) of the *Wwft BES* in conjunction with Section 7(1) and Annex B of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
54 Section 2.10(1) of the *Wwft BES*. Cf. Section 1.8 of the *Wwft BES*.

2.10.2 Cases of higher risk

A service provider itself determines whether a situation is high-risk (and hence requires enhanced customer due diligence) by means of a risk assessment. In their risk assessment service providers must take account of the list of (non-exhaustive) risk factors referred to in the *Wwft BES* and the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation (see below). These factors guide service providers in their assessment of whether a situation is high-risk. The stated examples are not exhaustive, however; there may also be other factors indicating high risk. Service providers draw up policy and procedures on the basis of their risk assessment and identify cases in which there is high risk.

The *Wwft BES* specifies at least the following cases:[55]

- Correspondent bank
- Customer not physically present
- Geographic area with higher risk
- Company with higher risk
- Transactions with higher risk
- Unusual circumstances

Correspondent bank

A credit service provider that enters or has entered into a corresponding banking relationship must ensure that:[56]

a. it gathers sufficient information on the credit service provider concerned to obtain a comprehensive view of its business operations and, based on information in the public domain, assesses the credit service provider's reputation and the quality of the supervision to which it is subject
b. it assesses that credit service provider's procedures and measures in place to prevent money laundering and terrorist financing
c. in the case of a new correspondent banking relationship, the decision to enter into that relationship is taken or approved by individuals authorised to do so by the credit service provider
d. the responsibilities of both credit service providers are recorded in writing
e. the credit service provider concerned has identified the customer and verified their identity and also continually monitors customers that have direct access to payable-through accounts and that the service provider concerned is capable of providing the relevant customer data at the request of the credit service provider that enters into a correspondent banking relationship.

55 Section 2.10(1) of the *Wwft BES* in conjunction with Section 7(3) and Annex D of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
56 Section 2.11 of the *Wwft BES*.

Customer not physically present

If a customer is not physically present to have their identity verified, the service provider must take measures to offset the higher risk. A service provider must determine whether the declared identity actually matches the identity of the person presenting himself.

The following options are available:[57]

a. verifying the customer's identity on the basis of additional documents, data or information
b. checking the authenticity of the submitted documents
c. ensuring that the first payment related to the business relationship or transaction is made to or from an account belonging to the customer with a credit service provider established in the countries of the Kingdom of the Netherlands, the United States of America or Canada.[58]

Geographic area with higher risk

The following areas pose a higher risk of money laundering or terrorist financing:[59]

a. countries identified by credible sources, such as mutual assessments, detailed evaluation reports or published follow-up reports, as not having effective AML/CFT systems;
b. countries identified by credible sources as having significant levels of corruption or other criminal activity;
c. countries subject to sanctions, embargoes or similar measures imposed by, for example, the European Union or the United Nations;
d. countries funding or supporting terrorist activities or having organisations classified as terrorist operating on their territory.

A customer resident or established in such a country poses a higher risk of money laundering or terrorist financing. The same applies in the case of a customer having a UBO established in one of the aforementioned areas.

Service providers must take additional measures to mitigate the increased risk. If the customer is not a natural person, it is up to the service provider to take steps to ascertain the customer's legal status. Special measures must also be taken for transactions and business relationships associated with these areas, such as additional checks on business relationships or limiting or refusing to execute certain transactions. This is recorded during the customer acceptance procedure.

57 Section 2.10(2) of the *Wwft BES*.
58 Section 2.10(2)(c) of the *Wwft BES* in conjunction with Section 3 of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
59 Section 2.10(1) of the *Wwft BES* in conjunction with Section 7(3) and Annex D(1b) and (3) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.

Company with higher risk

The following situations indicate higher risk:[60]

a. legal entities or legal structures that are personal asset-holding vehicles
b. companies that have nominee shareholders or shares in bearer form
c. businesses that are cash-intensive
d. the company's ownership structure appears unusual or excessively complex given the nature of its business activity.

Good practice

In the policy the service provider specifies which situation poses increased risk. This involves the following ten points at a minimum:

- personal businesses with assets exceeding $250,000
- companies in which more than 25% of transactions are in cash
- companies having a structure comprising more than two layers.

Companies having nominee shareholders or shares in bearer form are not accepted as customers.

Transactions with higher risk

Transactions that typically carry a higher risk of money laundering or terrorist financing are:[61]

a. private banking;
b. products or transactions that facilitate anonymity;
c. transactions that take place, without certain safeguards, remotely or electronically and are not regulated, recognised, approved or accepted by the relevant national authorities;
d. payments received from unknown or unassociated third parties;
e. new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products;
f. transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance or of great scientific value, as well as ivory and protected animal and other species.

Unusual circumstances

If the circumstances surrounding the business relationship are unusual, this indicates a higher risk of money laundering or terrorist financing.[62]

60 Section 2.10(1) of the *Wwft BES* in conjunction with Section 7(3) and Annex D(1c), (1d), (1e) and (1f) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
61 Section 2.10(1) of the *Wwft BES* in conjunction with Section 7(3) and Annex D(2) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
62 Section 2.10(1) of the *Wwft BES* in conjunction with Section 7(3) and Annex D(1a) of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.

A service provider must take reasonable steps to investigate the background and purpose of complex or unusually large transactions, unusual transaction patterns and transactions lacking a clear economic or lawful purpose. In such cases, the entire business relationship with the customer should be subjected to enhanced CDD.

Good practice

After completing the customer due diligence, a service provider opens an account for a student. After a few weeks the student receives $60,000 on their account. The service provider investigates and finds that the student has taken out a loan of $60,000 'for studies' from a company involved in boat charters (not a customer of the service provider).

On closer examination the service provider cannot identify any relationship (economic, family) between the student and the boat charterer (or its UBO). The service provider files an unusual transaction report and raises the risk category to 'high'. As an additional measure every transaction on the student's account is examined before it is executed.

2.11 Recording of data

A service provider must record the data relating to the customer due diligence in an accessible manner.[63] The data must be retained for five years following termination of the business relationship or up to five years following the execution of the transaction.[64]

This concerns all data obtained during the customer due diligence and during the relationship, such as copies of identity documents, account information, correspondence, notes of discussions about and with the customer, transactions effected by the customer and other services provided for the customer. The file must also show how the decision-making process on customer acceptance took place, for example in the case of high-risk customers.

In the case of legal entities, records must include the particulars of the persons representing the legal entity vis-à-vis the service provider. In the case of the UBO, the person's identity and the method by which it was verified must be recorded. Where a customer acts as a trustee, the service provider must also record, in a retrievable way, the particulars of the settlors, the trustees and the UBOs. If the customer acts as a partner in an unincorporated partnership, the service provider must record the particulars

63 Section 2.13(1) of the *Wwft BES*.
64 Section 2.13(2) of the *Wwft BES*.

of the partners, the persons authorised to manage the partnership and the persons who are able to exert considerable influence on or have considerable interests in the partnership.

The following particulars must be recorded in all cases:[65]

a. name, address, place of residence/establishment of:
   i. the customer
   ii. the UBO
   iii. the person in whose name the deposit or account is held
   iv. the person who will have access to the safe deposit box
   v. the person in whose name a payment or transaction is executed
   vi. as well as their representatives
b. the nature, number, date and place of issue of the document used for identification purposes[66]
c. the nature of the service provided
d. in the case of:
   i. the depositing of securities, banknotes, coins, currency notes, precious metals and other assets:
      - the deposit number
      - the market value represented by these items at the time of deposit, or in the absence of a market value the amount that they represent, calculated according to other generally accepted valuation principles, or if the amount represented by these items cannot reasonably be determined, an accurate description of them.
   ii. the opening of an account:
      - a clear description of the type of account
      - the number allocated to the account
   iii. rental of a safe deposit box: the number or another distinctive reference of the safe deposit box concerned
   iv. payments made to redeem coupons or comparable documents of bonds or similar securities:
      - the amount involved in the transaction
      - the account number
   v. issuance of a life insurance policy: the number of the account from which the premium is paid
   vi. payment of a life insurance benefit: the number of the account to which the payment is made
   vii. entering into an obligation to make a payment for the holder of a credit card to the party who has accepted the presentation of that credit card as a means of payment, issuing credit cards or managing

65 Section 2.13(1) in conjunction with Annex B of the *Wwft BES*.
66 It is not mandatory to retain a copy of a passport or identity document, for example. The service provider can also note and retain the details of the document (ECLI:NL:CBB:2017:235).

credit cards, which is deemed to include in any case the effecting of payment transactions by credit card: the credit card or debit card number and the expiry date, or the cheque number and the corresponding bank account number

viii. execution of money transactions: the credit card or debit card number and expiry date, or the cheque number and the corresponding bank account number

ix. offering an opportunity to compete for prizes and awards as part of the operation of games of chance including gaming casinos: the nature, origin, purpose, size and other unique characteristics of the assets or items concerned

x. providing trust services: the identity of the companies, legal entities or similar bodies involved.

2.12 Assessment and classification of customer

A service provider must draw up a risk profile for every customer with whom it has a business relationship.[67] This risk profile includes the expected transaction profile. This is important for the ongoing monitoring of the business relationship and the transactions conducted during that relationship in order to ensure that they match the service provider's knowledge of the customer and the risk profile. Service providers can only detect unusual transactions if they have adequate knowledge of the customer concerned. If individual transactions show that a customer is deviating from the profile, the service provider must evaluate the consequent risks.

Service providers must allocate their customers to risk categories, which must include at least the following:

- low risk[68]
- higher risk[69]
- normal risk
- unacceptable risk

2.13 Within risk tolerance?

On the basis of the customer due diligence and the defined risk profile, a service provider may conclude that an existing or intended relationship with a customer poses excessive integrity risks. The customer due diligence procedure may also fail, for example due to a lack of necessary information, leaving the service provider unable to determine precisely who its customer is and/or what the purpose of the proposed business relationship is and whether the intended service is appropriate.

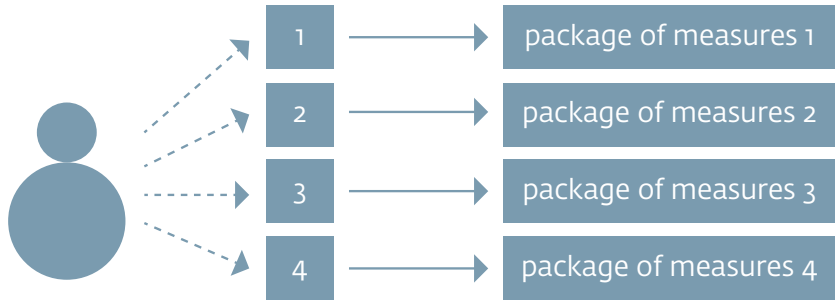
67 Section 2.5 of the *Wwft BES*.
68 Section 2.8 of the *Wwft BES*.
69 Section 2.10 of the *Wwft BES*.

Examples of unacceptable risks

- Problems in verifying the identity of the customer or the UBO.
- Customers who wish to remain anonymous or who provide fictitious identity details.
- Shell banks (banks incorporated and licensed in a jurisdiction where they have no physical presence).
- Customers appearing on a sanctions list.
- Customers who, combined with the products they wish to acquire, present unacceptable risks, for example on the basis of additional information.
- Customers who are unwilling to provide full information (or are unable to provide adequate documentation to verify such information) concerning their nature and background, the purpose of the business relationship and in particular the source of the customer's funds.
- The customer's organisational structure or the purpose of the structure of which the object company is a part is found upon examination to be complex or non-transparent, given the nature of the customer's activities, without there being a logical commercial explanation for this.
- Professional counterparties who lack the required licence, referred to as 'illegal financial undertakings'.
- Customers that give the service provider insufficient information concerning structures, cash flows and/or tax motives.

2.14 Allocating a level of control

The *Wwft BES* is risk-based. This also means that the level of control must match the customer's risk profile. The level of control relates, for example, to the frequency of the periodic review and the intensity of the ongoing monitoring.



In cases where the service provider believes there is a higher risk of money laundering or terrorist financing, the service provider must take additional measures (if these are not already being applied). The possible measures include the following:

- additional checks of business relationships and correspondent relationships;
- limiting or not executing transactions;
- a deeper examination of the rationale for transactions and the source of the funds;
- mandatory second-line advice;
- 'bad press' monitoring.

The service provider must record in its policy which level of control is appropriate for a given risk. The chosen level of control for a customer is recorded.

2.15 Refusal of a customer

A service provider must carry out the customer due diligence before the business relationship is entered into or a one-off transaction is executed. A service provider is not permitted to enter into a business relationship or execute a transaction if it has not performed customer due diligence or if the customer due diligence has not resulted in:[70]

- identification and verification of the customer and UBOs;
- an understanding of the customer's ownership and control structure;
- determination of the purpose and intended nature of the business relationship;
- identification and verification of the party representing the customer; and
- clarity on whether the customer is acting on their own behalf or for a third party.

A service provider may thus conclude on the basis of the customer due diligence that an existing or potential customer carries excessive risk of involvement in money laundering or terrorist financing. It can also occur that the customer due diligence procedure cannot be conducted in full, for example due to the lack of necessary customer information, and the service provider cannot therefore determine precisely who its customer is and/or what the purpose of the intended business relationship is. In these cases the service provider will not enter into a business relationship with the customer or will terminate an existing business relationship and execute no transactions.

In order to ensure that this obligation is fulfilled, the service provider includes in its customer acceptance policy the conditions under which a relationship with the customer will be refused (see also §2.13) and when this will lead to the reporting of an unusual transaction to FIU-NL (see below).

2.16 Intended unusual transaction?

If the service provider has indications that an actual or potential customer is involved in money laundering or terrorist financing, it is required to notify the Financial Intelligence Unit (FIU-NL).[71] See also *Potentially unusual transaction?* in this Good Practices document.

The service provider must also notify the Financial Intelligence Unit – the Netherlands (FIU-NL) of the refusal/non-acceptance of a customer if the customer due diligence has not provided the required information and there are indications of involvement in money laundering or terrorist financing.[72]

70 Section 2.4(1) and (2) of the *Wwft BES*.
71 Section 3.5 in conjunction with Section 3.4 of the *Wwft BES* in conjunction with Section 6 in conjunction with Annex A of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.
72 Section 3.5(4) of the *Wwft BES*.

3 Transaction monitoring

Click here to access flowchart

3.1 Transaction monitoring

Service providers are required to conduct ongoing monitoring of the business relationship and the transactions effected during that business relationship.[73] The aim of transaction monitoring is to identify unusual transactions and transaction patterns. If there are grounds for assuming that an actual or intended transaction is linked to money laundering or terrorist financing, the service provider must file an unusual transaction report with FIU-NL. To this end it is crucial that service providers have in place an effective transaction monitoring process.

The service provider can implement the transaction monitoring process on a risk basis as it sees fit. The process may include pre-transaction monitoring, post-event transaction monitoring or a combination of both.

In order to define its transaction monitoring process, the service provider must weigh up the costs, risks and the method it intends to use. The process will depend greatly on the nature, scope and risks of the service provider's activities and the number of transactions it conducts on a daily basis. The law does not require transaction monitoring to be automated. It is therefore up to the service provider to decide whether monitoring should be manual or automated, but the decision must be well founded. Where there are larger numbers of transactions, automated transaction monitoring can be beneficial in terms of effectiveness, consistency and completion time, for example.

Transaction

The *Wwft BES* defines a transaction in broad terms as: "an act or combination of acts performed by or on behalf of a customer in relation to the purchasing or provision of services". This means that all information associated with the financial transaction data that becomes known to the service provider in the provision of the services can be included in the transaction monitoring.

The words "act or combination of acts performed by or on behalf of a customer" should be interpreted in such a way that the passive involvement of the service provider (by virtue of its knowledge of the transaction) can also trigger the statutory reporting obligation.

73 Section 2.2(2)(d) of the *Wwft BES*.

Good Practices – transaction monitoring

The key features of an appropriate transaction monitoring process are shown below.

1. Service providers must ensure that the transaction monitoring process reflects the risks of money laundering and terrorist financing that emerge from the SIRA. Service providers must also take account of expected transaction behaviour when determining the risk profile of the customer and/or 'customer peer groups'.
2. Service providers must have developed an adequate policy for transaction monitoring and have sufficiently elaborated this policy in underlying procedures and operating processes.
3. Service providers must have an (automated or manual) transaction monitoring process in place and have a substantiated and adequate set of business rules (detection rules with scenarios and threshold values) to detect money laundering and terrorist financing risks. Service providers must periodically test these business rules, with regard to both technical aspects and effectiveness.
4. Service providers must have an adequate alert notification and handling process in place. Service providers must ensure that they fully and immediately notify FIU-NL of any intended or executed unusual transactions. In this process, for each alert considerations and conclusions are documented underlying decisions to close or escalate an alert.
5. Service providers must have structured their governance with regard to transaction monitoring in such a way that duties are clearly segregated.
6. Service providers must offer their staff tailored training programmes. Staff must be aware of the money laundering and terrorist financing risks associated with transactions.

Non-compliance with the reporting obligation

Failure by a service provider to fulfil its reporting obligation or to do so on time – even unintentionally – constitutes a crime or an offence that may give rise to consequences.

3.2 Intended transaction

An intended transaction is a transaction that has not yet been executed. These are situations, for example, in which face-to-face contact takes place between a customer and the employee of the service provider, or in which a customer's instruction to execute a transaction is withdrawn without a plausible explanation.

Intended transactions can be monitored by means of pre-transaction monitoring.

3.3 Pre-transaction monitoring

Pre-transaction monitoring is carried out before the transaction is executed and mainly applies to situations involving face-to-face contact between the customer and the employee of the service provider. An example is when a customer visits a branch to exchange, remit or deposit cash at the counter. Pre-transaction monitoring may enable unusual transactions to be detected before or when they are executed.

Good practice

A bank observes that the products purchased in a transaction are unrelated to the customer's normal business. The transaction is put on hold and reported to the compliance officer. The compliance officer recommends making enquiries of the customer. The account manager's enquiries reveal that the customer has started a second line of business and is investing in it. Proof of this is provided. The transaction is then executed with the compliance officer's approval.

Good practice

A person visits a money remittance office to conduct a money transaction at the counter. The person pays in $1,200 but is known to be unemployed. The person cannot properly explain how they have come by the money, and the money remittance office decides not to execute the transaction.

3.4 Post-event transaction monitoring

In the case of post-event transaction monitoring the service provider has already executed the transaction and the transaction monitoring takes place retrospectively. The post-event transaction monitoring process depends greatly on the nature and size of the service provider and the number of transactions it conducts on a daily basis. The law does not require transaction monitoring to be automated. It is therefore up to the service provider to decide whether monitoring should be manual or automated, but the decision must be well founded.

Good practices in post-event transaction monitoring

The post-event transaction monitoring process comprises the following steps:

#	Step	Notes
1	Risk identification	During the identification process the service provider systematically analyses the money laundering and terrorist financing risks posed by various types of customers, products, distribution channels and transactions. It then documents the results of this analysis in the SIRA. The service provider then applies the SIRA to its policy, business processes and procedures relating to transaction monitoring. The identification and analysis of risks also requires the service provider to classify its customers into risk categories, such as high, medium and low, on the basis of the money laundering and terrorist financing risks posed by the business relationship with the customer. To determine a customer's risk profile, the service provider draws up a transaction profile based on the expected transactions or the expected use of a customer's product (or of a customer group's product by means of 'peer grouping'). By creating a transaction profile in this way the service provider can conduct sufficient monitoring to ensure that transactions effected during the relationship are consistent with its knowledge of the customer and the associated risk profile.
2	Detection of patterns and transactions	Service providers must have a transaction monitoring process in place to detect unusual transaction patterns and transactions that may indicate money laundering or terrorist financing. This can be done using a manual process or an automated post-event transaction monitoring system, depending on the nature and size of the service provider and the number of transactions it conducts on a daily basis. Before using the system the service provider must ensure that all source systems of the transactions to be monitored have been identified and the data have been fully and correctly included in the transaction monitoring process. This can be data concerning the customer, the services and the transactions.
3	Data analysis	The service provider analyses the transaction data, for example using a transaction monitoring system or specific, intelligent software. Automated transaction monitoring systems generate alerts based on business rules. An alert is a signal that indicates a potentially unusual transaction. The service provider investigates possible unusual transactions. The findings of the investigation must be adequately and clearly documented. If the investigation reveals that a transaction is unusual, the service provider must report it to FIU-NL without delay. The service provider must clearly explain and document its considerations and its decision on whether to report a transaction.
4	Assessment, measures and documentation	The service provider then assesses the consequences of the report to FIU-NL and any feedback from FIU-NL for the customer's risk profile and determines whether any additional control measures need to be taken. The final part of the transaction monitoring process is the retention of data obtained by the service provider from transaction monitoring. In this connection, the service provider retains the data relating to the unusual transaction report and records it in such a way that it is retrievable and the transaction can be reconstructed for five years after the report was filed.

Good practice – Transaction profile

A workable transaction profile must fulfil the following six criteria:

1. Current: the transaction profile is up-to-date and has a date. All relevant changes to the profile are made promptly.
2. Complete: the transaction profile contains all bank account numbers, names of beneficiaries and authorised representatives.
3. Specific: the expected items and money flows are clearly described in terms of e.g. amounts, services and frequency. The (threshold) amounts indicated are well substantiated and can actually contribute to recognising unusual transactions.
4. Clear: financial flows are represented in clear and simple diagrams.
5. Substantiated: the transaction profile is substantiated with relevant documents clarifying and explaining the forecast financial flows.
6. Documented: the transaction profile is documented in the customer file.

3.5 Potentially unusual transaction?

If the service provider encounters transactions that do not match the expected pattern and/or profile or serve no economic or legal purpose, it must investigate the background and purpose of these transactions. In so doing, the service provider must pay particular attention to unusual transaction patterns and transactions that typically carry a higher risk of money laundering or terrorist financing.

Indicators of unusual transactions

If a transaction matches certain indicators, the service provider must report it to FIU-NL. The law prescribes indicators for categories of service providers.

One subjective indicator applies to all service providers. The subjective indicator concerns a transaction in which the service provider has reason to assume that it may be related to money laundering or terrorist financing. Every service provider must assess whether a particular transaction should be reported because of a possible link to money laundering or terrorist financing. Service providers are individually responsible for the adequate reporting of unusual transactions.

In addition, objective indicators apply to each category of service provider. The objective indicators describe situations in which transactions must always be reported. The following objective indicators of unusual transactions have been defined for the following categories of service providers:[74]

74 Section 3.4 of the *Wwft BES* in conjunction with Section 6 in conjunction with Annex A of the Anti-Money Laundering and Anti-Terrorist Financing (BES) Regulation.

- credit institutions and money transaction offices:
  - A non-cash transaction for an amount exceeding USD 250,000.
  - A cash transaction for an amount exceeding USD 11,000.
  - A cash deposit of USD 11,000 or more to a credit card or prepaid card account.
  - The use of a credit card or a prepaid card in connection with a transaction of USD 11,000 or more.
  - A money transfer of USD 2,000 or more, unless it is a money transfer by a service provider that entrusts the settlement of the money transfer to another service provider that is also subject to the reporting obligation referred to in Section 3.5(1) of the *Wwft BES*.
- For life insurers (and insurance brokers):
  - Life insurance policies with a first or single premium payment exceeding USD 11,000.
  - Life insurance policies with a first or single premium payment exceeding USD 6,000 in cash.
  - If the first or single premium payment exceeds USD 140,000.[75]
  - A cash benefit payment exceeding USD 11,000.
  - A benefit payment exceeding USD 50,000 to an account at a bank outside the public bodies of Bonaire, Sint Eustatius and Saba within five years after the policy was taken out.[76]
- Credit card companies and credit institutions:
  - Cash deposit exceeding USD 2,000 in a credit card account by a customer in the public body of Bonaire, Sint Eustatius or Saba.
  - Use of credit card for transactions exceeding USD 11,000 to or from Bonaire, St Eustatius or Saba.
- Casinos:
  - Depositing of coins, banknotes and other items with a value exceeding USD 5,000.
  - Transactions exceeding USD 5,000.
- Trust offices:
  - All cash transactions exceeding USD 5,000 or the equivalent in foreign currency in which the person who has the reporting obligation is directly or indirectly involved.
  - Transactions of USD 50,000 and over including the purchase or cashing by the customer of cheques, traveller's cheques or similar means of payment.
  - Transactions of USD 500,000 and over involving cheques, traveller's cheques or similar means of payment.

75 For service e, Annex A of the Act.
76 For service f, Annex A of the Act.

Where indicators are related to a specific limit, the service provider must also assess whether there is a connection between two or more transactions. This can be done on the basis of the type of transaction and the amounts involved. If a connection is found to exist, these transactions could be reported under the subjective indicator.

The service provider records the findings of the investigation into the transaction (or intended transaction) in the customer file. The service provider also documents its considerations and its decision on whether to report a transaction. If a transaction is suspected of being linked to money laundering or terrorist financing, the service provider must report it to FIU-NL without delay.

3.6 Second-line assessment

We expect the service provider to have specified the advisory and other duties of the compliance function with regard to transaction monitoring, for example how the compliance function's advice on high-risk cases should be dealt with. The compliance function may also have a role in reporting unusual transactions to FIU-NL. We also expect quality assurance for transaction monitoring to be assigned to the compliance function.

3.7 Unusual transaction

If the findings of the investigation show that a transaction is unusual, and which indicator is applicable, the service provider must report it to FIU-NL without delay.[77]

It must also clearly explain and document its considerations and its decision on whether to report the transaction. In cases of doubt, the service provider should always report the transaction to FIU-NL.

3.8 FIU-NL

Service providers must report actual or intended unusual transactions to FIU-NL without delay once the unusual nature of the transaction becomes known.[78]

Confidentiality obligation

Service providers, and personnel working for them, must not disclose the fact that an unusual transaction has been reported, including to the customer that is the subject of the report.[79] Exceptions are possible in so far as they arise from the law. Violation of the confidentiality obligation is a criminal offence.

77 Section 3.5 of the *Wwft BES*.
78 Section 3.5 of the *Wwft BES*.
79 Section 3.10 of the Wwft BES.

Information to be submitted with an unusual transaction report

The *Wwft BES* lists the data to be submitted when reporting an unusual transaction. These data are vital for FIU-NL to be able to analyse an unusual transaction. If a service provider systematically fails to submit specific data, FIU-NL may report this omission to the supervisory authority, which in turn may issue an instruction to the service provider to develop internal procedures and controls for the prevention of money laundering and terrorist financing.

The *Wwft BES* lists the following data to be submitted when reporting an unusual transaction:[80]

a. the customer's identity, the identity of the ultimate beneficial owners and, where possible, the identity of the party on whose behalf the transaction is effected;
b. the nature and number of the customer's identity document and, where possible, of the identity documents of the other persons referred to in section (a);
c. the nature, time and place of the transaction;
d. the value, origin and destination of the funds, securities, precious metals or other assets involved in the transaction;
e. the circumstances that have led to the transaction being designated as unusual;
f. a description of the high-value items involved in the transaction;
g. additional data designated in a general administrative order.[81]

Indemnification

If an unusual transaction report has been submitted correctly, in good faith and in accordance with the requirements of the *Wwft BES*, indemnifications apply to the reporting service provider. The *Wwft BES* provides for criminal indemnification and civil indemnification.[82]

80 Section 3.5 of the *Wwft BES*.
81 At the time of publication of this Good practice, such general administrative order has not been adopted.
82 Sections 3.8 and 3.9 of the *Wwft BES*.

4. Customer review

Importance of up-to-date customer data → When must a customer review take place? → What does a customer review involve? → What is the result of the customer review?

4.1 Importance of up-to-date customer data

A service provider must take reasonable steps to ensure that the data gathered during the customer due diligence process are accurate and complete and kept up to date.[83]

Keeping customer data up to date is an integral part of the customer due diligence. In order to fulfil this obligation, a service provider can request a previously identified customer to supply updated information and documents.[84]

83 Section 2.2(6) of the *Wwft BES*.
84 *Parliamentary Papers II* 2019/20, 35 458, no. 3, p. 27.

4.2 When must a customer review take place?

An important reason for a customer review is that the customer file needs to be updated after a certain period has elapsed. This means in practice that the service provider must conduct periodic reviews of customer files. The frequency and the depth of such reviews are risk-based.

Furthermore, renewed customer due diligence is conducted in the following cases:[85]

- conspicuous and abnormal transaction behaviour;
- if a customer becomes part of a different or changed ownership or control structure;
- if there are indications that the customer is involved in money laundering or terrorist financing;
- if there is doubt as to the reliability of information previously obtained from the customer;
- if the risk of an existing customer's involvement in money laundering or terrorist financing provides grounds for a review – this means that where the risk is low the review frequency can be lower than in the case of customers with, for example, normal or increased risk.

4.3 What does a customer review involve?

The depth of the review depends on the risk. A review normally comprises the following elements:

- Check of sanctions, PEPs and 'bad press'.
- Analysis of the customer's transactions:[86]
  - Comparison of the actual transaction profile with the risk profile/ transaction profile drawn up at the time of onboarding, together with a more detailed analysis of the differences that lie, for example, outside a predefined range.
  - Checking whether transactions are consistent with the purpose and nature of the relationship.
  - Checking whether the transactions are consistent with the source of the funds used in the business relationship or the transaction.
  - Checking for any conspicuous transactions or transaction patterns in the transaction histories. It is possible to examine, for example, the amounts and cash transactions involved, any amounts transferred immediately to another account, the use of the accounts by third parties, unknown counterparties and commingling/pooling.
  - All transactions that are conspicuous and cannot be readily explained are analysed more closely. More detailed information may be obtained from the customer if necessary in order to carry out this analysis.

85 *Parliamentary Papers II* 2019/20, 35 458, no. 3, p. 27; Section 2.3 of the *Wwft BES*.
86 Section 2.2(2)(d) of the *Wwft BES*; Section 2.5 of the *Wwft BES*. Section 2.8(4) of the *Wwft BES*.

- Updating of customer data, including:[87]
  - Contact details
  - UBO details
  - Purpose and nature of the relationship
  - Source of funds
  - Transaction profile
- Updating of risk classification. The updating of the risk classification may naturally have consequences for the level of control.

4.4 What is the result of the customer review?

After the customer review the service provider has an up-to-date, well-documented customer file that meets the requirements. The service provider has also updated the risk classification.

The review may be grounds for terminating the relationship with the customer:

- A service provider may conclude on the basis of the review/customer due diligence that a customer poses excessive integrity risks. In that case the service provider will seek to terminate the relationship with the customer. This may occur at the start of the relationship, but also during the relationship, if internal and/or external developments place increased demands on the customer acceptance process.
- The customer due diligence conducted as part of the review may also fail, for example due to a lack of necessary information, leaving the service provider unable to determine precisely who its customer is and/or who the UBOs are and/or what the purpose of the intended business relationship is and whether the intended service is appropriate. It may also emerge that a PEP is involved, as a result of which the service provider requires additional information that the customer fails to provide.

If there is already a business relationship with the customer and the service provider cannot meet the customer due diligence requirements, the service provider will terminate the business relationship.[88] The service provider must draw up a customer exit policy to ensure that all these obligations are met and that relationships with existing customers are ended in an appropriate manner. Among other things, this policy will set out the circumstances under which the relationship with the customer will be terminated and the procedure to be adopted.

If the service provider ascertains on the basis of the review, in particular on the basis of the transaction analysis, that one or more transactions are unusual, the service provider must report them to FIU-NL as soon as their unusual nature becomes known.[89]

87 The customer's identity does not have to be verified again, unless there are doubts as to the reliability of the identity data supplied previously.
88 Section 2.4(3) of the *Wwft BES*.
89 Section 3.5 of the *Wwft BES*.