DNB *Wwft* Q&As and Good Practices

DeNederlandscheBank

EUROSYSTEEM

Contents

This document is published in both Dutch and English, in case of any discrepancies or interpretation differences between the documents, the Dutch text prevails.

1 Introduction

1.1 DNB's integrity supervision

In addition to solidity, integrity is a prerequisite for a sound and reliable financial system. Under the Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme – *Wwft*), De Nederlandsche Bank (DNB) carries out integrity supervision for a wide range of financial institutions: banks, life insurers, payment service providers and agents, electronic money institutions, crypto service providers[1], exchange institutions, trust offices[2], other financial institutions[3], and certain branch offices.[4] The primary purpose of our integrity supervision under the *Wwft* is to prevent the financial system from being used to facilitate money laundering or terrorist financing.

1 As referred to in Section 1a(4), under l and m, of the *Wwft*. The integrity supervision of crypto service providers will be taken over by the Dutch Authority for the Financial Markets (AFM) with the entry into force of the Markets in Crypto-Assets Regulation (MiCAR) on 30 December 2024.
2 Trust offices in particular are also subject to the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren 2018 – Wtt 2018*). As a result, they must meet additional requirements, which are not addressed in the present document.
3 Other financial institutions referred to in Section 1a(3) of the *Wwft*. The *Wwft* refers to parties other than banks whose principal business is performing one or more of the activities included in points 2, 3, 5, 6, 9, 10, 12 and 14 of Annex I to the Capital Requirements Directive (CRD).
4 These are branches of banks, payment service providers, electronic money institutions, exchange institutions, life insurers and other financial institutions located in the Netherlands as referred to in Section 1a(3), under a, of the *Wwft*.

1.2 Rationale, structure and future changes

1.2.1 Rationale for revising the Guideline on the *Wwft* and Sw and purpose of the DNB *Wwft* Q&As and Good practices (*Wwft* Q&As/GPs)

In 2011, on the recommendation of the Financial Action Task Force (FATF), DNB published the first version of the Guideline on the *Wwft* and Sw (hereinafter: the Guideline). The Guideline has undergone several partial revisions since then, most recently in December 2020. Evaluations by the FATF, the European Banking Authority (EBA) and the Council of Europe, the recommendations made in these evaluations, the DNB report "From recovery to balance", and discussions with private stakeholders (e.g. in the context of the National Forum on the Payment System and roundtable discussions with banks) have led us to decide on a comprehensive revision of the Guideline.

DNB's report "From recovery to balance" states that financial crime can be combated more efficiently and effectively if institutions and supervisors adopt a more risk-based approach[5], facilitated by the smarter application of data-driven technological innovations and more focused cooperation throughout the chain. Moreover, the roundtable discussions with banks revealed that, in practice, the Guideline is regarded as a standards framework with little or no room for individual interpretation. To correct this perception, this revision seeks to make the document less prescriptive. The Guideline has also been translated into a new policy statement, consisting of descriptions of the legal framework and overviews of relevant national and international policy statements, and complemented by rationales and examples in the form of Q&As and good practices[6]. Not every section contains a legal framework, rationale, Q&As or good practices.

- Q&As reflect our views on the implementation and application of legal standards, and are thus an interpretation of these standards. Institutions can comply with laws and regulations in other ways as well. However, they must be able to demonstrate and substantiate their compliance if they choose to do so.
- Good practices set out suggestions or recommendations. They are examples of how institutions can comply with legislative and regulatory requirements that, in our opinion, provide a good interpretation of the obligations arising from laws and regulations. Institutions are free to adopt another approach, as long as they comply with the relevant laws and regulations, and are able to demonstrate this on reasoned grounds.

With the *Wwft* Q&As/GPs, we aim to provide an up-to-date document that:

- gives institutions a convenient overview of their obligations under the *Wwft*;
- supports institutions in designing proportional risk management structures;
- offers guidance on the application of a risk-based approach to customer due diligence and ongoing monitoring; and
- leaves room for innovative applications.

In this context, the *Wwft* Q&As/GPs underline the goal of the *Wwft*: to ensure that gatekeeper institutions prevent the financial system from being used for money laundering or terrorist financing. The measures taken by institutions should contribute to that goal – and thus are not an end in themselves. The *Wwft* also imposes obligations on institutions that leave no room for a risk-based approach (such as the reporting obligation, confidentiality obligation and retention obligation). Institutions must comply with these obligations in full.

5 See Section 1.5.
6 The Explanatory guide to DNB's policy statements identifies four types of policy statements: a supervisory regulation, a policy rule, a Q&A and a good practice. Each type of policy statement has its own status. For more information about this, please consult the Explanatory guide to DNB's policy statements on our Open Book on Supervision page.

1.2.2 Structure of the *Wwft* Q&As/GPs

This document is structured as follows: Chapter 2 discusses risk management and training. After that, Chapters 3 and 4 deal with customer due diligence, with Chapter 3 focusing on initial customer due diligence and Chapter 4 discussing ongoing monitoring. Chapter 5 looks at proper data recording, retention obligations and the protection of personal data, and Chapter 6 covers a number of miscellaneous topics.

1.2.3 Future changes to the *Wwft* Q&As/GPs

There are a number of ongoing developments that are expected to result in updates to this document in the future. One such development is the revision of the European AML/CFT framework. This document does not yet anticipate that revision, but is based on the laws and regulations in force at the time of publication, as there will likely be a multi-year implementation period after the new framework is published. There may also be other reasons to amend this document. Thematic examinations and signals we receive from institutions can lead to new Q&As or good practices, for example. The *Wwft* Q&As/GPs will therefore be reviewed and updated with some regularity. Thanks to the document's structure, it will not be necessary to revise it in its entirety, as individual parts can be changed without affecting the rest of the text.

1.3 Status of other DNB policy statements on integrity supervision

The *Wwft* Q&As/GPs replace the Guideline as far as the sections dealing with the *Wwft* are concerned. The Sw section of the Guideline remains in force and will not be amended. Given the modernisation of the Dutch sanctions regime, we have chosen to exclude the Sw from the scope of the *Wwft* Q&As/GPs. Guidance on the Sw will be published separately on our website. Once the modernisation of the Dutch sanctions system has become sufficiently concrete, this will be revised.

Besides the Guideline, we have published several other policy statements on integrity legislation. An overview of all our general and sector-specific policy statements on integrity legislation is available on our Open Book on Supervision page.[7]

1.4 Legal framework

1.4.1 Relevant national and international laws and regulations

Our integrity supervision is mainly based on the *Wwft*. The *Wwft* implements the European directive aimed at preventing money laundering and terrorist financing (AMLD).[8] This European directive, in turn, is partly based on the recommendations of the FATF, the organisation that develops policies to combat money laundering and terrorist financing worldwide. In addition to the *Wwft*, our integrity supervision is based on the Financial Supervision Act (Wet op het financieel toezicht – Wft), the Pensions Act (Pensioenwet), the Mandatory Occupational Pension Scheme Act (Wet verplichte beroeps-pensioenregeling) and the Act on the Supervision of Trust Offices 2018 (Wet toezicht trustkantoren 2018 – Wtt 2018) (hereinafter collectively: integrity legislation).[9] This policy statement, however, is mainly concerned with the *Wwft*. We also conduct integrity supervision under the Sw.

In interpreting and applying the *Wwft*, institutions must also comply with related laws and regulations. The European Wire Transfer Regulation 2 (WTR2) and the General Data Protection Regulation (GDPR) are particularly relevant in this context. The WTR2 specifies the information that must be included in transfers of funds in order to clarify their origin and destination. At the end of 2024, it will be replaced by the Transfer of Funds Regulation

7 https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-themes/supervision-of-financial-crime-prevention-integrity-supervision/
8 Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ 2015 L 141/73), as subsequently amended.
9 We also conduct integrity supervision of institutions in the Caribbean Netherlands. This supervision is subject to other laws and regulations.

(TFR). Although the WTR2 falls outside the scope of the *Wwft* Q&As/GPs, we would like to emphasise the importance of the obligations arising from it. We also refer to our policy statements on the WTR2 and other relevant laws and regulations, available at our Open Book on Supervision. For more information on the obligations arising from laws and regulations for which we have not been designated as the competent authority, we refer to the relevant competent authority. For example, the competent authority for the GDPR is the Dutch Data Protection Authority.

1.4.2 International policy statements

Several international policy statements are relevant to the interpretation and application of the *Wwft*, including those issued by the EBA and the FATF. The EBA's policy statements are particularly significant with regard to the implementation of the *Wwft*. The European legislator has mandated the EBA to develop AML/CFT policies and support their effective implementation. The EBA has also been tasked with monitoring the implementation of policies and standards to identify vulnerabilities. In addition, the EBA leads, coordinates and oversees the AML/CFT efforts of all financial institutions and competent authorities in the European Union.

The EBA has issued several relevant guidelines, opinions, reports and other statements. Together with the other European authorities represented in the EBA's various bodies, we are involved in the development of these policy statements and will take them into account in our supervision. The purpose of the EBA guidelines is to ensure the consistent and uniform application of standards under European legislation in all EU Member States. The guidelines are addressed to supervisors and, in some cases, also directly to institutions, but do not have the same status as binding European regulations (such as directives and regulations). Guidelines provide guidance on the implementation and application of European regulations, and supervisors and institutions must make every effort to comply with them.[10] This also means that we will refer to EBA policy statements where relevant.

The EBA's policy statements are published on its website. Many of these EBA policies were published recently, or have recently been updated. They therefore contain new or revised information compared to what was available when the previous Guideline was published. We expect institutions to take these sources into account in the design and application of their anti-money laundering and anti-terrorist financing policies, procedures and measures to ensure effective management of the risks they identify. Where relevant international policy statements exist, we refer to these rather than include information from them in our own guidance. This ensures that institutions can always consult recent sources.

1.4.3 National guidance documents and policy statements

The *Wwft* Q&As/GPs are a guide for DNB-supervised institutions and exist alongside the General Guidance issued by the Ministry of Finance and the Ministry of Justice and Security. The General Guidance also clarifies the statutory obligations arising from the *Wwft* and provides compliance tools. It should be read in conjunction with the *Wwft* Q&As/GPs. In addition, several other *Wwft* supervisors have published guidance documents for the institutions under their supervision, such as the Dutch Authority for the Financial Markets' (AFM) Guidance on the *Wwft* and Sw.

10 Guidelines are subject to a "comply or explain" requirement, which means that supervisors such as DNB must indicate whether they include them in their supervision. In our periodically updated overview "Application of the Guidelines and Recommendations of the European Supervisory Authorities", available at Open Book on Supervision, we set out which guidelines we take into account in applying the relevant supervisory laws and regulations (Application of the Guidelines and Recommendations of the European Supervisory Authorities).

1.5 Risk-based approach

Given the importance of the risk-based approach, we briefly discuss its background and our views on it below.

1.5.1 Background to the risk-based approach

The risk-based approach is a cornerstone of the authoritative FATF standards, which form the basis of European regulations.[11] The FATF expects both institutions and supervisors to take measures to prevent money laundering and terrorist financing that are appropriate to the risks identified. In its standards, the FATF provides examples of how this approach can be applied in practice. The AMLD prescribes a risk-based approach as well.

This risk-based approach also plays a central role in the *Wwft*, which implements the AMLD. The *Wwft* stipulates that the institutions themselves are responsible for taking measures to identify risks of money laundering and terrorist financing. Based on this risk assessment, they must then decide which mitigation measures to apply. The *Wwft* also requires institutions to consistently align their customer due diligence with the risk sensitivity to money laundering or terrorist financing of all types of customers, business relationships, products or transactions. Institutions must be able to demonstrate that their customer due diligence measures are proportionate to the money laundering or terrorist financing risks identified. The higher the risk posed by the customer, the more scrutiny is called for; if the risk is lower, less intensive monitoring will suffice.

1.5.2 DNB's perspective on the risk-based approach

The public expects financial institutions not to be involved in financial crime. Compliance with laws and regulations and maintaining public trust are first and foremost the responsibility of the institutions themselves. This responsibility extends from the workfloor up to the highest levels of management.

DNB ensures that financial institutions take appropriate measures to avoid becoming involved in financial crime. For example, we expect directors to know, understand and control the integrity risks faced by their institution. Robust lines of defence, starting with institutions' commercial units and under the ultimate responsibility of the board, are essential.
The risk-based approach also forms the basis of our supervision in this context: we deploy our supervisory capacity in areas with the highest integrity risks. The intensity of our supervision increases as the potential materialisation of risks has greater implications for public trust in the sector. Our approach is aligned with the EBA's guidelines on risk-based supervision.

In the report "From recovery to balance", about the role of banks, we set out our expectations regarding the risk-based approach in more detail. A more risk-based approach can enhance the efficiency and effectiveness of efforts to combat financial crime. Enhancing effectiveness primarily means that less criminal money will find its way into the financial infrastructure, while enhancing efficiency will reduce the administrative burden on banks and their customers.

11 See: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

A risk-based approach means that banks need to have more information about higher-risk customers in order to assess the risk and implement the most appropriate controls. Taking more limited measures for low risks creates scope to focus resources on higher risks, making it possible to deploy scarce resources precisely where the best results can be achieved. Interpreting the *Wwft* too strictly can cause institutions to take disproportionate measures, placing an unnecessary burden on their customers. This can potentially undermine the effectiveness of the *Wwft* while also eroding support for compliance and hindering supervision. To ensure an effective and efficient risk-based approach to integrity risks, it is therefore essential that institutions are highly aware of the relevant risks.

1.6 Financial inclusion

In line with the risk-based approach, we emphasise the importance of financial inclusion and avoiding the unnecessary exclusion of customers (de-risking). Bona fide customers should be able to access essential financial services. Our position on this issue is consistent with that of the Ministry of Finance, the Ministry of Justice and Security,[12] the EBA and the FATF: compliance with integrity obligations should not result in the financial exclusion of legitimate customers. The integrity legislation framework is sufficiently flexible to allow financial institutions to meet their obligations effectively without excluding customers or even customer groups.

12 *Parliamentary Papers II, 2022-2023, 31 477, no. 80.*

2 Risk management and training

This chapter discusses the institution's risk management (see Section 2.1) and the training and screening of its employees and day-to-day policymakers (see Section 2.2).

Risk management is the institution's framework for managing the money laundering and terrorist financing risks it faces. First, the institution must identify relevant risk factors and assess the money laundering and terrorist financing risks it is exposed to due to its business model and operations (see Section 2.1.1). The institution then uses this company-wide risk assessment to establish guidelines, procedures and measures (policy) to effectively manage and mitigate risk (see Section 2.1.2). This policy should cover the institution's interpretation of and compliance with its customer due diligence obligations, its obligation to report to FIU-NL, and its record keeping and retention obligations. The day-to-day policymakers, the compliance function and the audit function have various roles, duties and responsibilities in this process (see Section 2.1.3).

In complying with the obligations under the *Wwft*, it is important that the institution's employees and day-to-day policymakers receive training so that they are familiar with the provisions of the *Wwft*, and to ensure that they are screened (see Section 2.2).

2.1 Risk management

2.1.1 Risk identification and assessment (company-wide risk assessment)

Legal framework

Company-wide risk assessment

The *Wwft* stipulates that institutions must take measures to identify and assess risks of money laundering and terrorist financing (the risk assessment). These measures must be proportionate to the nature and size of the institution in question. In identifying and assessing *Wwft* risks, an institution must consider the risk factors relating to its specific types of customers, products, services, transactions and supply channels, as well as to the countries or geographic territories it operates in. The *Wwft* also requires institutions to document the results of their risk assessment. In addition, they must keep their risk assessment up to date and make the results available to the supervisor upon request.

The EBA's ML/TF Risk Factors Guidelines provide further guidance on how an institution can fulfil the obligation to conduct a risk assessment, how to keep it up to date and how to document the results. More information on how to design a risk assessment can be found in the DNB Integrity Risk Analysis Good Practices.

The EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer further clarify the different roles, duties and responsibilities of the management body and the compliance function with regard to risk assessment. See also Section 2.1.3.

The aforementioned EBA guidelines also provide further guidance on the group-level risk assessment.

Relationship between risk assessment and SIRA

The Decree on Prudential Rules for Financial Undertakings (Besluit prudentiële regels Wft – Bpr) lists several types of institutions that must ensure a systematic analysis of integrity risks. The SIRA focuses on reputation risks and financial risks due to inadequate compliance with laws and regulations. It therefore has a broader scope than the *Wwft* risk assessment, which deals with the risk of money laundering and terrorist financing. If an institution is also required to conduct a SIRA, it makes sense to include the *Wwft* risk analysis in the SIRA, but this is not mandatory.[13]

The following laws and regulations are particularly relevant:

- Section 2b of the *Wwft*

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- EBA Guidelines on the role and responsibilities of the AML/CFT compliance officer
- DNB Integrity Risk Analysis Good Practices

Rationale

A sound risk assessment is crucial to prevent involvement in money laundering and terrorist financing. Institutions conduct a risk assessment to understand and gain insight into which parts of their operations are exposed to money laundering and terrorist financing risks. This should enable them to shape their policy, in the form of guidelines, procedures and measures, in such a way that it can mitigate and manage the risks they are exposed to.[14]

13 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 43.
14 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 43.

Good practices

Good practice: customer portfolio analysis

An institution conducts an analysis of its business strategy and customer portfolio to determine its exposure to customer groups, sectors or geographical areas that pose an inherently higher risk with regard to money laundering or terrorist financing. The results of this analysis are used in the risk assessment.

Good practice: risk information from external sources

To identify risks as part of its risk assessment, an institution consults relevant external sources, taking into account the EBA's ML/TF Risk Factors Guidelines. These relevant external sources can be publications from international organisations, governments, supervisors and industry associations. Examples include the European Commission's Supranational Risk Assessment (SNRA), the National Risk Assessment (NRA) and publications by bodies such as the FATF and the Anti Money Laundering Centre (AMLC). The institution uses this information, where relevant, in preparing and updating its risk assessment.

Good practice: updating the risk assessment

Taking into account the EBA's ML/TF Risk Factors Guidelines, an institution has established a process to ensure that it draws lessons from incidents, FIU-NL reports and thematic analyses, and that these are used in the periodic update of the risk assessment. The institution also ensures that major incidents lead to an immediate update of the risk assessment. In this process, each function contributes to proper risk assessment based on its own role, as defined in the design of the risk assessment. These roles may change when the risk assessment is updated.

2.1.2 Guidelines, procedures and measures (policy)

Legal framework

Guidelines, procedures and measures

The *Wwft* requires institutions to have guidelines, procedures and measures (policy) in place to mitigate and effectively manage the risks identified in their risk assessment (see Section 2.1.1), and in the most recent versions of the SNRA and NRA.

This policy should be proportionate to the nature and size of the institution. It should at least cover compliance with the provisions of the *Wwft* with regard to the institution's risk management, groups, customer due diligence, the obligation to report to FIU-NL, the record keeping and retention obligations, and employee screening and training. The *Wwft* also requires institutions to ensure a systematic review of the policy and, where necessary, its adjustment. When the risk assessment is updated, the institution's policy should also be updated where necessary.[15]

15 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 44.

Several EBA guidelines provide further guidance on how to interpret the obligation to draft, review and update ML/TF policy (see below).

This policy must be approved by the institution's day-to-day policymakers. More generally, the EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer provide further guidance on how to invest the various roles, duties and responsibilities with regard to the policy within the institution. See also Section 2.1.3.

Group policy

The *Wwft* also stipulates that an institution that is part of a group must effectively apply the guidelines and procedures applicable at group level (group policy) within its own organisation, insofar as that group policy complies with the *Wwft*. The institution must also ensure the effective application of this group policy by its branches or majority subsidiaries registered outside the Netherlands. If the law of a third country prevents this, the institution must ensure that the branch or majority subsidiary takes additional measures. The group policy should at least cover information security and intra-group information sharing, insofar as the information relates to the prevention of money laundering and terrorist financing. The EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer provide further guidance on group policies.

The following laws and regulations are particularly relevant:

- Section 2c of the *Wwft*
- Section 2f of the *Wwft*
- Commission Delegated Regulation (EU) 2019/758 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards on the minimum action and type of additional measures that credit and financial institutions are required to take to reduce the risk of money laundering and terrorist financing in certain third countries

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- EBA Guidelines on the use of remote customer onboarding solutions
- EBA Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services
- EBA Guidelines on the role and responsibilities of the AML/CFT compliance officer

Q&As

Question

Should an institution eliminate all risk of involvement in money laundering or terrorist financing?

Answer

No, institutions are expected to take all reasonable measures to prevent their involvement in money laundering or terrorist financing. At the same time, the use of a risk-based approach also means accepting that some criminal money will flow through the financial system, despite mitigation measures. Institutions are not expected to prevent this completely, so there is an accepted "residual risk".

Good practices

Good practice: designing policy

When adopting and amending policies, an institution considers whether they:

- are appropriate to the money laundering and terrorist financing risks the institution is exposed to. This means that policies must properly consider:
  - the various interests and goals with regard to the mitigation measures to be deployed;
  - the intensity of the measures taken to comply with the *Wwft*, depending on the risk. Measures should be applied less intensively for lower risks and more intensively for higher risks.
- pay sufficient attention to other interests, such as the protection of personal data and access to the financial system.

Good practice: mitigation measures in case of conspicuous use of cash

An institution has a customer whose conspicuous cash use cannot be explained on the basis of the customer profile, which means that there is an increased risk. The institution takes measures to mitigate this risk. Its policy stipulates the following:

- engage with the customer about their conspicuous use of cash and give them a chance to provide an explanation.
- use understandable language to communicate to the customer why the measures that are being taken are necessary, how the customer's explanation has been taken into account and, if applicable, what the customer can do to have the measures rescinded.
- ensure that the mitigation measures are specific and proportionate, and give the customer sufficient time to change their operations.
- ensure that the mitigation measures do not unnecessarily impede the legitimate use of cash.
- a cash withdrawal or deposit limit may be used as a targeted control for individual customers. The institution is aware that using this control could have major consequences for the customer and only does so in exceptional cases, if the increased money laundering or terrorist financing risk persists after investigation and customer contact. This may be the case if the customer initially fails to cooperate with the investigation, if the information provided by the customer is insufficient to explain the cash usage, or if the control is necessary to manage integrity risks and there is no less impactful alternative. The institution must periodically assess whether the limit is still necessary. It must also do so if the circumstances change.

Good practice: additional measures policy

An institution's policy states that it must apply the following additional measures for higher-risk customers:

- More frequent reviews of the business relationship.
- Deeper investigation into the rationale behind transactions, and into the origin of funds.
- Mandatory advice from the compliance function on accepting or continuing the business relationship.
- Additional research using public sources to determine if there has been any negative press about the customer.

The policy on research using public sources was drafted in consultation with the data protection officer to strike the right balance between managing the risk of money laundering and protecting personal data.

Good practice: risk tolerance policy

In its policy, an institution has defined when customers fall within or outside its own risk tolerance. If a customer falls within the risk tolerance and should not be refused under the *Wwft*, the institution accepts them and, if necessary, takes appropriate mitigation measures based on the customer's risk profile. In drafting its policy, the institution observes the EBA's Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services. This also means that the institution strives to ensure that potential customers are not unnecessarily prevented from accessing financial services.

Good practice: customer communication policy

An institution considers the customer's point of view in drafting its policy. It recognises that customers may not understand why they have to provide information and cooperate in customer due diligence, and that they may feel reluctant to do so. They also might not understand why the institution has to take mitigation measures.

The institution pays special attention to this in its policies, and in its communication with customers. For example, the institution ensures that customers receive a clear explanation as to why certain information is requested or why certain mitigation measures are taken.

2.1.3 Duties and responsibilities of policymakers, and of the compliance and audit functions

Legal framework

Day-to-day policymakers and members of the supervisory authority

The *Wwft* stipulates that if an institution's day-to-day policy is set by two or more persons, one of these policymakers must be responsible for the institution's compliance with the *Wwft* (*Wwft* policymaker). The *Wwft* also requires guidelines, procedures and measures (policy) to be approved by the day-to-day policymakers. The EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer further clarify the duties and responsibilities of the day-to-day policymakers, the *Wwft* policymaker and the members of the supervisory authority.

Compliance function

Pursuant to the *Wwft*, an institution must have an independent and effective compliance function (if appropriate given its nature and size). The Explanatory Memorandum to the *Wwft* makes it clear that the way in which the compliance function is set up can be aligned with the nature and the size of the institution. It also states that, as a matter of principle, persons involved in performing the compliance function should not also be involved in the activities they supervise, in order to ensure independence. For smaller institutions, however, it can be disproportionately burdensome to ensure the independence of the compliance function in this way. The Explanatory Memorandum also states that an institution may choose to outsource the compliance function (either in its entirety or in part).[16]

With regard to the duties and responsibilities of the compliance function, the *Wwft* stipulates that it must focus on monitoring compliance with the law, the internal rules drawn up by the institution itself, and the obligation to report to FIU-NL. The EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer provide further guidance on the duties and responsibilities of the compliance function.

16 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 44.

Audit function

If appropriate given its nature and size, an institution should ensure that it has an independent audit function. The audit function monitors compliance with the *Wwft* and the performance of the compliance function. The intensity of the audit function should be aligned with the institution's risk profile. The level of independence of the audit function should be appropriate to the nature and size of the institution.[17] Like the compliance function, the audit function can also be outsourced (in its entirety or in part).[18]

The following laws and regulations are particularly relevant:

- Section 2c(3) of the *Wwft*
- Section 2d of the *Wwft*

The following other policy statements are particularly relevant:

- EBA Guidelines on the role and responsibilities of the AML/CFT compliance officer
- EBA Guidelines on internal governance (where applicable)

Q&As

Question

Are smaller institutions required to have an independent *Wwft* compliance function?

Answer

For smaller institutions, maintaining an independent *Wwft* compliance function may be disproportionately burdensome and therefore inappropriate. The size and type of the institution also play an important role with regard to this requirement.

Good practices

Good practice: compliance framework

An institution has defined the design, operation and importance of its compliance function in a compliance framework. This stipulates, among other things, that the compliance function must have access to all relevant information, rooms and persons within the organisation. It also stipulates who the compliance function reports to and that the compliance function has direct access to the supervisory board. In drawing up this framework, the institution used the EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer.

Good practice: duties and responsibilities of the first line

An institution's policy clearly sets out the duties and responsibilities of the three lines of defence. It clearly describes that the first line is primarily responsible for identifying, assessing and managing money laundering and terrorist financing risks in its day-to-day operations. The policy also states that first-line employees should integrate the *Wwft* requirements into their business decisions and daily tasks.

Good practice: compliance policy

An institution's compliance function discovers that one of its departments is not in full compliance with its policy, exposing the institution to undesirable money laundering risks. The compliance function discusses this with the department's management. Afterwards, it submits a report to the department's management, setting out the agreed actions. The *Wwft* policymaker and the audit function also receive this report.

17 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 45.
18 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 17.

In consultation with management, a meeting is convened in which the compliance function provides feedback on the findings to employees, and in which management emphasises the importance of the agreed actions. The compliance function monitors the follow-up of the agreed actions and reports on this to the department's management. It also includes its findings in the standard monitoring report to the *Wwft* policymaker.

Good practice: audit function

An institution considered the following points when it set up its audit function:

- The audit function must operate independently.
- The audit function must assess compliance with the *Wwft* and the performance of the compliance function at least once every year.
- The audit function must document its findings.
- The institution must use these findings to tighten its controls where necessary. The audit function should then determine whether these interventions are sufficient.

2.2 Education and training

Legal framework

The *Wwft* requires institutions to ensure that their employees and day-to-day policymakers are familiar with the provisions of the *Wwft*. This obligation applies as relevant to the performance of their duties, taking into account the risks, nature and size of the institution. In addition, institutions must ensure that employees and day-to-day policymakers undergo periodic training so they are able to identify unusual transactions and conduct sound and complete customer due diligence. Training programmes must be tailored to the institution's risks, nature and size as well.

Institutions must also ensure that their employees and day-to-day policymakers are screened as relevant to the performance of their duties, taking into account the risks, nature and size of the institution. The screening authority Justis offers employee screening guidelines on its website.[19]

The following laws and regulations are particularly relevant:

- Section 35 of the *Wwft*

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- EBA Guidelines on the role and responsibilities of the AML/CFT compliance officer

Good practices

Good practice: education & training

An institution has tailored its training offering to the different roles of its employees:

- Analysts learn how to conduct sound and complete customer due diligence. During their training, they also learn about the new and existing sources they must use and the timely detection of red flags. The course also pays attention to awareness of potential biases and how to deal with them.
- Employees who have direct contact with customers, for example in customer acquisition or sales, receive training to make them aware of the *Wwft* provisions relevant to their role so that they can apply this knowledge in their work.
- Senior, specialist, management and executive first-line staff receive additional training to keep abreast of developments related to money laundering or terrorist financing risks, as well as of legislative and regulatory developments.

19 https://www.justis.nl/en/products/certificate-of-conduct/documents-certificate-of-conduct

- Compliance function staff also receive additional training to keep abreast of developments related to money laundering or terrorist financing risks, as well as of legislative and regulatory developments.
- Day-to-day policymakers receive training that helps them effectively manage their ultimate responsibility.

The institution bases the content of its courses partly on case studies that are relevant to its operations. Besides offering mandatory e-learning modules and on-site training, the institution organises regular knowledge sessions where money laundering techniques, methods and trends are discussed, and where employees can discuss specific cases. To enable staff to keep up with new developments and to improve awareness in the long term, the institution regularly provides training courses.
The institution regularly evaluates and revises the content of its courses to reflect changes in integrity risks, controls, laws and regulations.

The institution documents its training offering, which courses have been completed, how frequently courses are taught and who has taken which courses. This enables it to assess, monitor and respond to the organisation's knowledge level on an ongoing basis.

Good practice: training programme

An institution has an annual training programme for its first-, second- and third-line staff. Besides legislative and regulatory developments, the emphasis in these programmes is on real-life cases: practical examples related to money laundering and terrorist financing and how the institution dealt with them.

The training sessions thus link practical experience, legislation and regulations to policy, procedures and the underlying work processes. Through these training programmes, the institution offers employees clear guidelines on how to act in various situations.

Good practice: staff screening

Before hiring new employees, an institution assesses their reliability. The institution's procedures and measures focus on:

- Establishing the candidate's identity;
- Checking the accuracy and completeness of the information and references provided by the candidate;
- The candidate's ability to provide a certificate of good conduct for a specific position.

The institution keeps the documents and the assessment report on file.

3 Customer due diligence: initial customer due diligence

This chapter discusses initial customer due diligence. Initial customer due diligence refers to all due diligence obligations prior to entering into (or not entering into) a business relationship with a customer or carrying out a non-recurring transaction. The subsequent ongoing monitoring of the business relationship and the transactions carried out during the course of the relationship is covered in Chapter 4.

By conducting customer due diligence, an institution finds out who it is doing business with. Institutions must conduct their customer due diligence using a risk-based approach. This does not mean that they can decide to skip it: customer due diligence must be carried out at all times.[20] The nature of the investigation must be demonstrably tailored to the customer and the risks identified by the institution.[21] When assessing the risk posed by a business relationship or non-recurring transaction, an institution must consider the relevant risk factors. Based on this individual risk assessment, the institution can then apply simplified, standard or enhanced customer due diligence measures. If the customer is expected to have a low risk profile, the institution can opt for simplified customer due diligence (see Section 3.2). For medium risk profiles, the institution must apply standard customer due diligence (see Section 3.1), while high-risk customers require enhanced customer due diligence (see Section 3.3). The institution may either outsource part of the customer due diligence process to a third party (see Section 3.4) or rely on customer due diligence performed by another institution (see Section 3.5).

20 Under certain circumstances, if an institution enters into a business relationship or conducts a transaction involving electronic money, it does not need to conduct initial customer due diligence.
21 Section 3(8) of the *Wwft*.

The institution must record the data it collects during customer due diligence (see Chapter 5). Ultimately, the institution must draw up a customer risk profile based on the information collected during the customer due diligence process and individual risk assessment. Based on this risk profile, the institution then determines whether the customer can be accepted or should be refused (see Section 3.6). If the institution accepts the customer, their risk profile becomes the basis for ongoing monitoring (see Chapter 4).

The *Wwft* states that an institution must conduct customer due diligence to prevent money laundering and terrorist financing.[22] This allows the institution to:

- Identify the customer and verify their identity (see Section 3.1.1);
- Establish whether the natural person representing the customer is authorised to do so and, where relevant, to establish this natural person's identity and verify it (see Section 3.1.2);
- Take reasonably required measures to verify whether the customer is acting on its own behalf or on behalf of a third party (see Section 3.1.3);
- To identify the customer's ultimate beneficial owners (UBOs) and take risk-based and appropriate measures to verify their identity and, if the customer is a legal person, take risk-based and appropriate measures to gain an understanding of the ownership and control structure of the customer (see Section 3.1.4);
- Establish the purpose and the intended nature of the business relationship (see Section 3.1.5);
- Monitor its business relationships and the transactions conducted during their existence on an ongoing basis so as to ensure that these match its knowledge of its customers and their risk profiles (see Chapter 4), where necessary carrying out further investigations into the origin of the funds used in the relevant business relationship or transactions (see Section 3.1.6).[23]

The *Wwft* also stipulates when an institution must conduct customer due diligence. It must do so in the following situations:

- If it enters into a business relationship in or from the Netherlands;
- If it carries out, in or from the Netherlands, a non-recurring transaction on behalf of a customer that amounts to at least €15,000, or multiple related transactions that together amount to at least €15,000;
- If there are indications that the customer is involved in money laundering or terrorist financing;
- If the institution doubts the truthfulness or completeness of data previously submitted by the customer;
- If the risk of an existing customer's involvement in money laundering or terrorist financing gives cause to do so.
- If there is an increased risk of money laundering or terrorist financing due to the country in which a customer is domiciled, resident or registered;
- If it carries out, in or from the Netherlands, a non-recurring transaction on behalf of a customer or trust constituting a transfer of funds as referred to in Section 3(9) of the WTR2, amounting to at least €1,000.[24]

3.1 Standard customer due diligence

3.1.1 Customer identification and identity verification

Legal framework

The *Wwft* requires institutions to identify their customers and to verify their identity. A customer is a natural or legal person with whom a business relationship is entered into or who has a transaction carried out. A business relationship is a professional or commercial relationship between an institution and a natural person, legal person or partnership firm, which is related to the professional activities of the institution and is expected to continue for a certain period from the moment the relationship is entered into. A transaction is an act or a combination of acts performed by or on

22 Section 3(1) of the *Wwft*.
23 Section 3(2) of the *Wwft*.
24 Section 3(5) of the *Wwft*.

behalf of a customer of which the institution has taken note in the provision of its services to that customer.

To identify a customer, an institution asks them to declare their identity, which it then verifies to confirm that the customer's declared identity matches their true identity. This is done on the basis of documents, data or intelligence from reliable and independent sources. The *Wwft* Implementation Decree (Uitvoeringsregeling *Wwft*) provides a non-exhaustive list of documents that can be used to verify a customer's identity. Examples include a valid identity card or passport, or, for legal entities, an extract from a trade register. The EBA's ML/TF Risk Factors Guidelines provide further guidance on identification and verification. The EBA's Guidelines on the use of remote customer onboarding solutions provide further guidance on the use of technological solutions, such as eID tools, to verify a customer's identity.

The following laws and regulations are particularly relevant:
- Section 1 of the *Wwft*
- Section 3(2), under a, of the *Wwft*
- Section 11 of the *Wwft*
- Section 4 of the *Wwft* Implementation Decree
- eIDAS Regulation[25]

The following other policy statements are particularly relevant:
- EBA ML/TF Risk Factors Guidelines
- EBA Guidelines on the use of remote customer onboarding solutions
- ESAs' Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process

Rationale

By establishing and verifying the customer's identity, the institution ensures that it knows who it is doing business with. This is also an important requirement in the risk assessment process.

Question

Is a name-number check sufficient to verify the customer's identity?

Answer

In itself, a name-number check, for example by transferring 1 cent, is not sufficient for identity verification. If a name-number check is used, one or more independent and reliable sources must be used as well.

Good practices

Good practice: policy on the reliability of sources

In its policy, an institution has defined which documents and what kind of intelligence or data are acceptable for the purpose of customer identity verification, and why. The institution also takes into account that certain documents may or may not be recognised by law as means of identification in the customer's state of origin. In drafting its policy, the institution used its company-wide risk assessment. The policy shows that the institution has conducted an analysis to determine which sources are reliable and independent.

25 Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC.

Good practice: policy on remote identification and verification

An institution uses remote customer acceptance solutions. It takes into account the fact that non-physical presence of the customer is considered a potentially higher risk under Annex III of the AMLD.

The institution has established policy on the use of these solutions for remote customer acceptance. In drafting this policy, the institution considered the EBA's Guidelines on the use of remote customer onboarding solutions. The policy covers the following topics:

- situations in which remote customer acceptance solutions can be used, taking into account the institution's company-wide risk assessment;
- an indication of which steps are autonomous and which steps require human intervention;
- the assessment process that precedes the introduction of a new remote customer acceptance solution;
- ongoing monitoring of the solutions;
- information gathering and data recording;
- ICT and security risk management.

The institution recognises that remote acceptance does not necessarily mean that the customer in question is high risk.

3.1.2 Representation

Legal framework

When a natural person acts as a representative of a customer, an institution must determine whether this person is authorised to do so. This is the case, for example, when a natural person acts as a director of a legal entity[26], or when a natural person acts as a representative of another natural person.

The identity of the natural person acting as representative must also be verified.

The following laws and regulations are particularly relevant:

- Section 3(2), under e, of the *Wwft*

The following other policy statements are particularly relevant:

- EBA Guidelines on the use of remote customer onboarding solutions

Good practices

Good practice: mapping the chain of representative authority

The representatives of legal entities are often the board members. When a natural person claims to indirectly represent a legal entity, the chain of representative authority must be mapped as well, for example using an extract from the trade register or the legal entity's articles of association. This allows the institution to determine whether the natural person is an authorised representative.

3.1.3 Acting on behalf of a third party

Legal framework

Institutions should take reasonable measures to verify whether a customer is acting on their own behalf or on behalf of a third party.

If it is clear that a customer is acting on behalf of another person, the other person also qualifies as a customer, meaning that the customer due diligence obligations arising from the *Wwft* also apply to this person.

26 *Parliamentary Papers II*, 2011-2012, 33 238, no. 3, p. 13.

The following laws and regulations are particularly relevant:

- Section 3(2), under f, of the *Wwft*

Good practices

Good practice: straw man risk

An institution has established indicators that point to a straw man risk: a concealment scheme in which a person pretends to act on their own behalf but in fact acts on behalf of criminal third parties. It uses these indicators in its customer due diligence. Examples of indicators include instances where a person is unable to answer certain questions, for example about the origin of funds, or where someone give vague and unclear reasons for a transaction.

If the institution suspects that the customer is a straw man for criminal third parties, this is treated as an unacceptable risk. The institution also reports the customer to FIU-NL.

3.1.4 Ultimate beneficial owner (UBO) & pseudo-UBO

Legal framework

UBO

The *Wwft* stipulates that institutions must identify their customers' ultimate beneficial owners (UBOs) and take reasonable measures to verify their identity. This obligation does not apply to listed companies that are already subject to disclosure requirements[27], or to wholly-owned subsidiaries of such companies.

The UBO is the natural person who ultimately owns or controls a customer, or the natural person on whose behalf a transaction or activity is carried out. The *Wwft* Implementation Decree specifies which categories of natural persons must in any case be regarded as UBOs in private liability companies, public liability companies, /religious organisations, other legal entities (including foundations and associations), partnerships (including general partnerships) and trusts. For many legal entities, under the implementation decree, a natural person qualifies as a UBO if they directly or indirectly hold more than 25% of the shares, voting rights or ownership interest. This 25% rule is meant to be indicative.[28] Persons with smaller interests may also qualify as UBOs if they have ultimate control by other means, such as contractual relations.[29]

Pseudo-UBOs

If, after exhausting all possible means and provided that there are no grounds for suspicion of money laundering or terrorist financing, no UBOs have been identified or there is some doubt as to whether the persons identified are UBOs, the customer's senior executives must be designated as UBOs ("pseudo-UBOs"). For the purpose of identifying pseudo-UBOs, senior executives are all members of the management board or all partners (except partners by way of financial backing). This also applies to non-executive directors on a one-tier board.[30]

An institution must document the measures it has taken and the difficulties it encountered during the verification process. If an institution cannot identify any UBOs or pseudo-UBOs, or if there are grounds for suspicion, it is obliged under Section 5 of the *Wwft* to refuse or terminate the provision of services, as the customer due diligence requirements cannot be met.[31]

27 These are disclosure requirements as laid down in Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, OJ 2004, L 390, or comparable disclosure requirements of a state outside the European Union; Bulletin of Acts, Orders and Decrees 2018, 241, p. 30.
28 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 4.
29 Bulletin of Acts, Orders and Decrees 2018, 241, p. 28.
30 Bulletin of Acts, Orders and Decrees 2020, 339, p. 19.
31 Bulletin of Acts, Orders and Decrees 2018, 241, p. 29.

Consulting UBO register[32] and feedback obligation

When entering into a new business relationship with a legal entity, institutions are obliged to consult the trade register (which includes the UBO register) to determine whether the customer's UBOs are registered. A similar obligation will apply in the future[33] when entering into a business relationship with a trust or similar legal structure, requiring institutions to consult the UBO register for trusts[34]. When performing customer due diligence, institutions must not rely exclusively on this information.

The *Wwft* also includes a so-called "feedback obligation".[35] If an institution determines that the UBO or pseudo-UBO details in the UBO register are incorrect or incomplete, it must report this to the Chamber of Commerce. This obligation does not apply if, under Section 16 of the *Wwft*, a report is made to FIU-NL. If no UBO is registered even though the legal entity or structure is required to register its UBOs,[36] the feedback obligation does not apply. The lack of registration does constitute a barrier to entering into a new business relationship.[37]

It is expected that the UBO register for trusts and similar legal structures will also be subject to a feedback obligation. However, this section of the act has not yet entered into force at the time of publication of this policy.[38]

Insight into ownership and control structure

If a customer is a legal entity, the institution must take reasonably required measures to gain an understanding of the ownership and control structure. If a customer acts as a trustee or on behalf of another legal structure, the institution must take reasonable measures to gain an understanding of the ownership and control structure of the trust or legal structure.

The following laws and regulations are particularly relevant:

- Section 1 of the *Wwft*
- Section 3(2), under b(15), of the *Wwft*
- Section 4(2) of the *Wwft*
- Section 10c of the *Wwft*
- Section 3 of the *Wwft* Implementation Decree

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act, issued by the Ministry of Finance and the Ministry of Justice and Security

Rationale

Individuals who want to bring criminal funds into the financial system or those who want to use funds for terrorist purposes can hide behind a legal entity or a complex corporate structure. It is therefore vital that institutions know who they are dealing with and understand the ownership and control structures of their customers, and that they know the identity of the natural persons on whose behalf transactions or activities are performed.

32 At the time of publication of this policy statement, access to the Dutch UBO register for legal entities is temporarily restricted for institutions following the Court of Justice's ruling of 22 November 2022, C-37/20 and C-601/20. The UBO register for trusts cannot be accessed either.
33 This specific article from the Act Implementing the Registration of Ultimate Beneficial Owners of Trusts and Similar Legal Structures (*Implementatiewet registratie uiteindelijk belanghebbenden van trusts en soortgelijke juridische constructies*) has not yet entered into force.
34 There is both a UBO register for legal entities and a UBO register for trusts and similar structures.
35 At the time of publication of this policy statement, the feedback feature is not yet fully accessible. For more information on submitting feedback and the current status, please consult the Chamber of Commerce website.
36 Not all legal entities are required to register UBOs under the Trade Register Act (*Handelsregisterwet*). For more information, visit the Chamber of Commerce website.
37 *Parliamentary Papers II*, 2021-2022, 32 545, no. 168, p. 5 and *Parliamentary Papers II*, 2021-2022, no. 3981.
38 Section 16 of the Act Implementing the Registration of Ultimate Beneficial Owners of Trusts and Similar Legal Structures.

Q&As

Question
Should identity documents always be requested to meet the verification requirement?

Answer
No, the institution must take reasonable measures to verify the UBOs' identity. "Reasonable measures" are those appropriate to the risk level. The goal is that the institution knows who the UBO is, and that it has sufficient reliable information about their identity, appropriate to the risk level. For example, the EBA's ML/TF Risk Factors Guidelines allow institutions to accept information provided by the customer to verify the identity of UBOs in carrying out simplified customer due diligence.

Question
At what level should pseudo-UBOs be determined in case of a layered structure?

Answer
If the institution identifies senior executives as pseudo-UBOs, the pseudo-UBOs are determined at the level of customer's legal entity. In some cases, the customer's director may be a legal entity. This legal entity does not qualify as a pseudo-UBO, as this must always be a natural person. If the director is a legal entity, any natural person acting as a director of that legal entity must be designated as a pseudo-UBO of the customer.[39]

Question
Can an institution enter into a business relationship with a customer if there is a discrepancy between the information the institution has on the customer and the UBO register?

Answer
If an institution detects a discrepancy between the information it has on a customer and the UBO register, it can still enter into a business relationship with the customer, unless there are indications of money laundering or terrorist financing, or customer due diligence cannot be completed.[40] The outcome of the institution's own customer due diligence is the most important factor in this context.

Good practices

Good practice: UBOs in structures with entities in high-risk jurisdictions

A customer has a complex, multi-layered company structure. Some entities in the ownership and control structure are located in high-risk jurisdictions. Given the risks identified for this customer relationship, the institution does not accept the customer's self-reported list of UBOs as sufficient evidence. The institution takes reasonable measures to map the customer's ownership structure (e.g. using trade register extracts, UBO register extracts (where possible) and additional sources) and identifies three individuals with more than 25% indirect formal control as UBOs. The institution then verifies the identity of these UBOs based on certified copies of identity documents. It documents its findings (the sources, analysis and conclusions) in the customer file.

39 *Parliamentary Papers II*, 2019-2020, 35 179, no. C, p. 13.
40 See also the General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act, issued by the Ministry of Finance and the Ministry of Justice and Security.

Good practice: identifying UBOs based on level of control

Customer due diligence reveals that a natural person with no formal position in the customer's organisation is able to exercise significant influence. This person has the power to block important decisions, such as strategic business decisions and major financial decisions. The institution designates this person as a UBO by virtue of their effective level of control.

Good practice: UBO of publicly owned company

An institution serves a company whose shares are formally all held by a public official. The institution determines that this public official does not personally hold the shares, nor do they personally have effective control. Share ownership and the resulting control is not linked to the natural person themselves, but to the position they hold (e.g. minister or mayor). There is nothing else to indicate that the official has personal ownership or control. The official's term of office is limited, and their successor will take over formal ownership of the shares. Moreover, the official cannot take binding decisions on behalf of the customer; only the company's board can do so. The institution therefore concludes that there are no natural persons who are UBOs by virtue of ownership or effective control and designates the customer's senior executives as pseudo-UBOs. The institution documents the measures it has taken and the difficulties it encountered during the verification process.

Good practice: direct and indirect share ownership

An institution has a customer that is part of a larger structure. The institution determines that none of the customer's direct shareholders hold more than 25% of the shares. When it investigates the company's structure, however, the institution identifies an individual who has several interests through multiple companies. This person directly holds 15% of the customer's shares, but also holds 50% of the shares in a parent company that holds 50% of the customer's shares. As a result, this person indirectly owns 25% of the customer's shares, in addition to the 15% they own directly. This brings their total stake to 40%. The institution identifies this person as a UBO based on the fact that they own more than 25% of the customer's shares.

Good practice: policy on identifying and verifying UBOs of EU customers

An institution has included the following in its policy on EU customers:

- For low- and medium-risk customers, a UBO's identity can be verified on the basis of a statement from a correspondent bank in an EU Member State and a copy of an identity document signed by the correspondent bank.
- For high-risk customers, a UBO's identity can be verified on the basis of a notary statement and a certified copy of an identity document.

Good practice: identifying and verifying UBOs for low-risk customers

An institution has a low-risk customer. It requests an extract from the UBO register, which shows that the company's shareholders are two natural persons who each own 50% of the shares. Upon the institution's request, the customer confirms that the UBOs listed in the register are in fact its UBOs and that their stated identity matches their actual identity. The institution has sufficient understanding of the customer's ownership and control structure and designates the two shareholders as UBOs. This completes the process of identifying and verifying the UBOs.

Good practice: identifying pseudo-UBOs for low-risk customers

An institution classifies a legal entity seeking to become a customer as low-risk. The institution is unable to identify a UBO based on its investigation of the prospect's ownership and control structure. The institution therefore identifies all senior executives (in this case the management board) of the legal entity as pseudo-UBOs and submits the relevant information from the trade register to the prospect's representative for confirmation. On behalf of the prospect, the representative confirms that the persons listed in the trade register are in fact the prospect's senior executives (and pseudo-UBOs) and that their stated identity matches their actual identity. The institution has no reason to doubt this. This completes the process of identifying and verifying the pseudo-UBOs. The institution documents the measures it has taken and the difficulties it encountered during the verification process.

Good practice: identifying pseudo-UBOs for high-risk customers

An institution has determined that a customer is high-risk, but there are no grounds for suspicion of money laundering or terrorist financing. Because the institution is unable to identify a UBO based on its documented investigation of the customer's ownership and control structure, it designates all senior executives as pseudo-UBOs. The institution requests the relevant information from the UBO register and asks the customer to submit an overview of its senior executives. The identity of these natural persons is verified on the basis of identity documents. Finally, the institution documents the measures it has taken and the difficulties it encountered during the verification process.

Good practice: identifying pseudo-UBOs in case of doubt

An institution notes that a legal entity it serves as a customer is owned by six individuals and that each of these individuals has an equal interest in the entity. This means that no single shareholder owns more than 25% of the shares. Because the shareholders received their shares from their father, the institution suspects that the father may be able to influence the company's operational management, despite the fact that he has no formal control. The institution is not sure whether the father should be designated as a UBO based on effective control. The account manager has several conversations with the family about this matter but finds no evidence that the father controls the company. Moreover, there are no indications that the customer is involved in money laundering or terrorist financing. The institution identifies the members of the customer's management board as pseudo-UBOs. It documents the measures it has taken and the difficulties it encountered during the verification process.

Good practice: unclear structures with entities in high-risk jurisdictions

A legal entity seeking to become a customer of an institution is part of a larger structure. The parent of this legal entity is based in a third country and has multiple subsidiaries in high-risk jurisdictions.

The institution investigates why the group to which the customer belongs uses this complex structure. This is not the first time that the institution has been faced with a complex international ownership and control structure, and it has a policy in place to determine when an internal or external expert opinion (for instance from a legal expert or tax specialist) should be sought regarding a customer's structure. In line with this policy, the institution asks the customer about the rationale for the structure and its operation. It also asks an expert to weigh in on the operation of the structure.

After reviewing the expert opinion, the institution concludes its investigation and finds that it still does not fully understand the customer's role in the structure. The institution determines that the customer due diligence process cannot be properly completed and therefore decides not to accept the customer.

3.1.5 The purpose and intended nature of the business relationship

Legal framework

The *Wwft* stipulates that customer due diligence must enable the institution to establish the purpose and intended nature of a business relationship. The institution must demonstrably match the intensity of its investigation of the purpose and intended nature of the business relationship to the money laundering or terrorist financing risk sensitivity of the type of customer, business relationship, product or transaction.

The EBA's ML/TF Risk Factors Guidelines provide further guidance on how to conduct a risk-based assessment of the purpose and intended nature of a business relationship.

The following laws and regulations are particularly relevant:

- Section 3(2), under c, of the *Wwft*

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines

Rationale

By establishing the purpose and intended nature of the business relationship, the institution gains insight into why the customer wants to use the service. This assists the institution in assessing the risks involved in providing the service to the customer.

Good practices

Good practice: asking customer about purpose and intended nature

It is not clear to an institution that primarily serves the Dutch market why a customer not based in the Netherlands is using its services or products. The institution questions the customer about this, assessing what this means for the customer's risk profile and whether the risk level is acceptable.

Good practice: assuming the purpose and intended nature for low-risk customers

Based on its risk assessment, an institution classifies a customer as low-risk. The product purchased by the customer has a specific application, such as a low-premium life insurance policy. The institution assumes the purpose and intended nature of the business relationship based on the product in question and the low risk involved, in line with the EBA's ML/TF Risk Factors Guidelines.
The institution does not carry out any further investigation.

Good practice: reference groups for determining purpose and intended nature

An institution may use reference groups (or peer groups) to establish the purpose and intended nature of a business relationship, if appropriate to its customer base. A reference group is a group of customers with at least some matching or similar characteristics. The institution can define these reference groups itself, but they should be sufficiently homogeneous. For example, "students using a student payment account" or "minors using a children's account" can be used as reference groups for a product such as a basic payment account. Another example of a possible reference group is a group of small business customers operating in the same low-risk sector within a certain turnover range and/or with low transaction volumes, such as homeowners' associations.

The institution can determine the purpose and intended nature of the relationship collectively for all customers within a reference group. The institution is not required to ask individual customers within a reference group about the purpose and intended nature of the business relationship before entering into a business relationship with them. Once the relationship has been established, however, the institution must periodically review whether the purpose and nature of the relationship with the customer still fits the reference group.

When using reference groups, the institution ensures that it is able to determine whether the right customers are being assigned to a reference group based on accurate and complete information. In addition, it periodically checks whether the customers belonging to the reference groups are still sufficiently homogeneous. If necessary, customers are moved to another reference group, for example because they no longer meet the characteristics of their reference group or fall outside the established ranges. The institution may also conclude that the customer can no longer be assigned to any reference group.

3.1.6 Source of funds

Legal framework

The *Wwft* provides that institutions should, if necessary, investigate the origin of the funds used in a business relationship or transaction. Whether such an investigation is necessary depends on the institution's assessment of the customer's risk level.[41]

The investigation into the origin of the funds can be limited to the funds used for the business relationship or transaction; the rest of the customer's assets can be disregarded.[42]

The following laws and regulations are particularly relevant:

- Section 3(2), opening words and under d, of the *Wwft*

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines

41 *Parliamentary Papers II*, 2011-2012, 33 238, no. 3, p. 12.
42 *Parliamentary Papers II*, 2011-2012, 33 238, no. 3, p. 12.

Rationale

Investigating the source of the funds helps institutions to understand the risks associated with providing services to customers, including the possibility that the institution may be facilitating criminal money flows. The risk assessment determines the measures an institution takes.

Good practices

Good practice: investigating the source of funds

In its policy, an institution has defined situations where desk research is sufficient to investigate the source of funds, as well as situations where more in-depth research is required. Examples of situations where – without additional risk factors – desk research could suffice include:

- A customer wants to open a savings account with a bank. The first deposit of €50,000 is transferred from the customer's bank account at another Dutch bank, which is the designated contra account. There are no known risk indicators for this customer.
- A customer who receives funds in their savings account for a planned and documented purchase, such as a holiday or wedding, where the customer uses the same savings account for each deposit and the amounts deposited are consistent with the savings target.
- A customer who transfers funds to a relative abroad for living expenses, where the customer has an established and known pattern of transfers with no suspicious activity.

Examples of situations where an in-depth investigation of the origin of the funds is needed:

- A customer who receives funds to make payments to third parties where the identity of the payee is not clear or where the payments are unusually large compared to the customer's previous transactions.
- A customer who receives a large amount of funds for international money transfers without a clear explanation of the origin of the money, especially if the transaction patterns are unusual for the customer.
- A customer who is involved in suspicious transactions or associated with persons or entities linked to criminal activity receives funds in a savings account.

Good practice: use of indicators

An institution identifies a number of indicators[43] to determine the level of scrutiny required when investigating the origin of funds. These include the amount being transferred, non-cash or cash form, the stated origin of the funds, the customer's occupation or business activities, the country of origin or destination of the funds, and the products or services provided.

43 In doing so, the institution can draw on the risk factors set out in Annexes II and III of the AMLD and the EBA's ML/TF Risk Factors Guidelines.

Good practice: documentary evidence for origin of funds

When investigating the origin of a customer's funds, an institution uses independent, reliable sources. Depending on the risk level, the institution may use certified copies of payslips, employer statements, a sales contract, overviews of share positions, wills, annual accounts or tax returns.

When requesting evidence, the institution takes into account the fact that some retention periods (e.g. for tax purposes) may have expired and that the customer may no longer be in possession of certain documents. If this is indeed the case, the institution considers whether the requested information is actually necessary given the level of risk, and whether it should ask the customer for alternative documents.

Good practice: questions on use of cash

An institution has a customer whose use of cash is conspicuous. Based on the information available to the institution, there is no logical explanation for this. The institution investigates the origin of the funds to determine whether the customer is involved in money laundering or terrorist financing. If necessary, the institution asks the customer questions to clarify the origin or destination of the cash. These questions are appropriate to the customer's risk level and may be informed by the following factors:

- the characteristics of the region in which the customer is located;
- the customer's sector or industry profile;
- location-related seasonal variations;
- large differences between the customer and relevant comparable customers.

After assessing the customer's answers, the institution determines whether any additional measures are required.

3.2 Simplified customer due diligence

Legal framework

If a business relationship or transaction due to its nature involves a low risk of money laundering or terrorist financing, simplified customer due diligence will suffice. In assessing the risk level, institutions must at least take into account the non-exhaustive list of risk factors set out in Annex II to the AMLD. The EBA's ML/TF Risk Factors Guidelines also describe sector-specific risk factors. Although the factors listed are potential indicators of lower risk, they do not guarantee low risk. Institutions must consider these factors in their risk assessment.

The *Wwft* does not specify what constitutes simplified customer due diligence. While the Explanatory Memorandum makes it clear that institutions must apply all customer due diligence measures even in the case of simplified customer due diligence, it also states that they can do so using a risk-based approach.[44] Customer due diligence should therefore also be carried out for low-risk customers, but the level of scrutiny can be tailored to the risk. The EBA's ML/TF Risk Factors Guidelines provide further guidance on how institutions can implement simplified customer due diligence.

In any case, an institution must have sufficient information to establish that a customer is low-risk and that simplified customer due diligence is sufficient, and to comply with the obligation to report unusual transactions. Even if an institution applies simplified customer due diligence, it must comply with Section 33(2) of the *Wwft*, which requires institutions to have the documents and information used for the customer due diligence process available on demand. This includes information on the legal entity, trust or similar structure and its UBOs, or on the natural persons concerned.

44 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 51.

The following laws and regulations are particularly relevant:
- Section 6 of the *Wwft*
- Section 16 of the *Wwft*
- Section 33 of the *Wwft*

The following other policy statements are relevant:
- EBA ML/TF Risk Factors Guidelines

Q&As

Question
Do customers that are covered by the *Wwft* themselves always pose a lower risk?

Answer
No, the fact that a customer qualifies as a *Wwft* institution does not automatically indicate a lower risk of money laundering or terrorist financing.[45] It may be a risk-mitigating factor, however, if used in a risk assessment that takes into account the type of institution, the nature of the products or services offered, the type of customer the institution serves, and whether the institution has the necessary licences to carry out its activities.

Good practices

Good practice: simplified customer due diligence policy

In its policy, an institution sets out when simplified customer due diligence can be used. This is determined on the basis of a preliminary risk analysis, taking into account risk factors for the identification of low-risk customers. In this risk analysis, the institution considers risk factors related to the customer, the products and services provided, transactions, delivery channels and geography. The institution updates its policy in response to incidents, FIU-NL reports and sector-wide developments, based on its latest insights.

It then applies simplified customer due diligence to customers it classifies as low-risk in accordance with this policy. In applying its policy, the institution substantiates that the relevant business relationship or transaction by its nature poses a lower risk of money laundering or terrorist financing. It also documents its substantiation and, if applicable, the evidence on which it is based.

Good practice: government institution as a customer

An institution uses the Government Organisations Register to confirm that a potential customer is a Dutch government institution.[46] Annex II to the Fourth Anti-Money Laundering Directive lists public institutions in EU Member States and third countries that have effective anti-money laundering and terrorist financing legislation and supervision as potentially lower-risk. Given that there are no other indicators that would warrant a medium- or high-risk classification, the institution uses simplified customer due diligence.

45 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 35.
46 The Government Organisation Register can be consulted on the government's website.

Good practice: listed company as a customer

An institution establishes that a potential customer is a company listed on the stock exchange of an EU Member State. Annex II to the AMLD notes that the transparency rules listed companies in the EU are subject to are an indicator of lower risk. The institution considers whether there are any other factors that could affect the risk level. In doing so, the institution takes into account the product, service or transaction purchased, the geographical risk factors associated with the customer, the percentage of marketable share capital, and whether the non-marketable portion is also subject to transparency requirements. The institution finds no factors indicating higher risk and uses simplified customer due diligence.

Examples of how simplified customer due diligence processes can be designed to meet specific obligations are provided in Sections 3.1 and 4.1.

3.3 Enhanced customer due diligence

Legal framework

The *Wwft* requires enhanced customer due diligence in the following cases:

- if a business relationship or transaction due to its nature involves a higher risk (see Section 3.3.1);
- complex or unusually large transactions, transactions that are part of an unusual pattern and transactions that have no clear economic or lawful purpose;
- transactions, business relationships and correspondent banking relationships involving states identified by the European Commission as higher-risk jurisdictions for money laundering and terrorist financing, which can also be referred to as high-risk third countries or HRTCs (see Section 3.3.2);
- when establishing correspondent relationships with respondent institutions in a third country involving payment transactions;
- in business relationships or transactions involving politically exposed persons (see Section 3.3.3).

The EBA's ML/TF Risk Factors Guidelines offer explanations and examples of how institutions can implement enhanced customer due diligence in each of the above cases, and for each sector where enhanced customer due diligence is required.

The following laws and regulations are particularly relevant:

- Section 8 of the *Wwft*
- Section 9 of the *Wwft*

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act, issued by the Ministry of Finance and the Ministry of Justice and Security

Good practice: correspondent banking

An institution with multiple correspondent relationships establishes a transaction profile before entering into a new customer relationship. This profile is based on input from one of the correspondent banks, insights into the institution's customer portfolio, the expected volume and the counterparties receiving the financial flows. The bank periodically checks whether the size and nature of the transaction flow still match the institution's original statements. In addition, the list of approved countries for correspondent relationships is reviewed annually and any relationship with a bank outside the EEA is approved by senior management.

3.3.1 Dealing with business relationships or transactions that, by their nature, carry a higher risk

Legal framework

Institutions must conduct enhanced customer due diligence if the nature of a business relationship or transaction represents an increased risk. The Explanatory Memorandum makes it clear that institutions should carry out a risk assessment to establish whether a higher risk is present prior to entering into a business relationship or executing a transaction.[47] In this risk assessment, institutions must at least take into account the non-exhaustive list of risk factors set out in Annex III to the AMLD. The EBA's ML/TF Risk Factors Guidelines also describe sector-specific risk factors.

The *Wwft* does not specify what enhanced customer due diligence entails for business relationships or transactions that by their nature represent a higher risk. The EBA's ML/TF Risk Factors Guidelines provide further guidance on how institutions can implement enhanced customer due diligence.

The following laws and regulations are particularly relevant:

- Section 8 of the *Wwft*

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- EBA report on ML/TF risks associated with payment institutions

Q&As

Question

Can an entire sector or group of customers with an elevated integrity risk automatically be classified as unacceptable?

Answer

The *Wwft* provides no basis for categorically labelling an entire sector or group of customers with similar characteristics as "unacceptable". Incidentally, it is also not possible to automatically classify customers operating in a low-risk sector as low-risk.

While there are sectors that are more vulnerable to integrity risks and therefore have a higher integrity risk profile, as discussed in the EBA's ML/TF Risk Factors Guidelines, this does not mean that all customers in these sectors should be assigned a high risk profile. All relevant factors should be considered in determining the risk profile. For example, the type of product sold by the customer should also be taken into account. In their risk assessments, institutions must at least take into account the risk factors listed in Annex III to the Fourth Anti-Money Laundering Directive.

The *Wwft* provides sufficient scope to avoid the unnecessary refusal of customers or transactions. Indeed, institutions can deploy adequate, customer-specific measures based on a customer-specific assessment.

47 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 53.

Question
Is cash always high-risk?

Answer
No, cash is legal tender that is used legitimately for day-to-day payments, and its legitimate use should not be impeded.

At the same time, research shows that cash can play an important role in money laundering or terrorist financing. The main reason for this is that cash is difficult to trace, making it an attractive means of payment for those seeking to disguise the origin of criminal assets. The use of cash by consumers and retailers can thus be an indicator of money laundering or terrorist financing. This is especially true if a customer's cash usage is conspicuously unusual and there are other risk-increasing factors.

Case law shows that it is common knowledge that various types of crime involve large amounts of cash, usually in high denominations. Transactions involving relatively high-denomination notes (e.g. €200 or €500) may indicate an increased risk of criminal activity. Although national banks in the euro area stopped issuing new €500 notes in January 2019, €500 notes are still in circulation. These notes are legal tender and must remain usable. Increased vigilance is warranted, however.

Good practices

Good practice: customer-specific risk factors

In its policy, an institution has defined which customer-specific risk factors can contribute to a higher risk, in accordance with the EBA's ML/TF Risk Factors Guidelines. These state that the institution should consider the following factors:

- Business or professional activities of the customer and ultimate beneficiary;
- Reputation of customer and ultimate beneficiary;
- Nature and behaviour of the customer and ultimate beneficiary.

Important considerations that the institution takes into account in the risk assessment include ties to sectors with a high risk of corruption or money laundering, involvement in sectors where large amounts of cash are used, political affiliations, prominent positions or public notoriety, compliance with disclosure requirements, and any frozen assets or negative media coverage that could damage the institution's reputation.

Good practice: conspicuous use of cash

Customers who use conspicuously large amounts of cash compared to their peers are given special attention in an institution's policy. One of the institution's customers is an online retailer with no brick-and-mortar presence that receives a lot of cash payments. It is unclear to the institution how an online retailer can receive cash payments. The institution has laid down in its policy that the conspicuous use of cash in combination with other risk-increasing factors requires additional investigation into the origin of these financial flows. It has established indicators to determine the appropriate depth of investigation into the origin of funds for cash deposits.

3.3.2 Politically exposed persons (PEPs)

Legal framework

A PEP is a person who holds or has held a prominent public position. Institutions must have appropriate risk management systems in place to determine whether customers or their UBOs are PEPs. The *Wwft* Implementation Decree includes a non-exhaustive list of prominent public positions. The Tax and Customs Administration has published a list of prominent public positions in the Netherlands.[48]

If a customer or UBO is a PEP, the institution must apply enhanced customer due diligence and take the following measures in addition to its standard customer due diligence when entering into or continuing a business relationship with the PEP or conducting a transaction for the PEP:

- obtain permission from a member of the institution's senior management;[49]
- take appropriate measures to identify the origin of the assets[50] and funds used in the business relationship or transaction;
- subject the business relationship to ongoing enhanced due diligence.

The institution must design these measures using a risk-based approach. This means that the intensity of the measures varies with the risk. The institution must always conduct customer due diligence.

The measures apply mutatis mutandis to family members and close associates of a PEP. The *Wwft* Implementation Decree further clarifies the concepts of family members and close associates of a PEP.

If the customer or UBO no longer holds a prominent public position, the institution must apply appropriate risk-based measures. The institution must do this for as long as necessary until the person in question no longer poses a higher risk due to their former PEP status, but at least for 12 months. The Explanatory Memorandum explains that potential risk factors that could be considered in this respect are the type of position previously held by the person in question, and the extent of the influence that the person could exercise after holding the politically prominent position.[51]

If an existing customer or UBO becomes or is found to be a PEP, the institution must take the additional measures without delay as soon as this becomes apparent.

The following laws and regulations are particularly relevant:

- Section 1 of the *Wwft*
- Section 8(5) to (9) of the *Wwft*
- Section 9a of the *Wwft*
- Section 2 of the *Wwft* Implementation Decree

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- List of prominent public positions in the Netherlands published by the Tax and Customs Administration

Rationale

Because of the potential corruption risks (and the attendant money laundering and reputation risks) associated with PEPs, the *Wwft* requires institutions to pay special attention to these individuals. It is important for institutions to know whether they are dealing with a PEP, as this enables them to identify and manage the risks associated with the customer more effectively.

48 *Wwft*: Prominent public positions in the Netherlands (belastingdienst.nl)
49 Senior management personnel is defined as follows: a. persons who determine the day-to-day policy of an institution; or b. persons working under the responsibility of an institution who fulfil a managerial role directly below the cadre of day-to-day policymakers, and who are responsible for natural persons whose activities affect an institution's exposure to money laundering and terrorist financing risks.
50 The EBA's ML/TF Risk Factors Guidelines explain that where "origin of the funds" refers to the funds used in the business relationship or non-recurring transaction, "origin of the assets" refers to the origin of the customer's total assets.
51 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 56.

Q&As

Question
Do PEPs by definition pose a high risk?

Answer
No, they do not. While the presence of a PEP in a customer's structure is a risk-increasing factor, it does not necessarily mean that the customer should be assigned a high risk profile. The *Wwft* does require institutions to take additional investigative measures for all PEPs. However, institutions can tailor the intensity of these additional measures to their risk assessment on a case-by-case basis. The risk level also depends on more factors than just PEP status.[52] For example, the children of a Dutch member of parliament with a basic payment account will usually be less risk-prone than the head of state of a country with an increased risk of corruption who wants to enter into a private banking relationship.

Good practices

Good practice: PEP screening policy

An institution has a policy on PEP screening. As part of this policy, the institution checks whether its customers or their UBOs qualify as PEPs both during customer acceptance and on an ongoing basis. PEP screening involves:

- Screening against general and "local" PEP lists, including lists of relevant positions.[53] The institution accesses these lists, which are periodically audited, through a subscription with an external service provider. PEP lists are also updated after certain events, such as elections.
- Internet research on customers and prospects with a public position (e.g. using the local trade register) to determine whether the public position should be classified as a prominent public position with the associated higher corruption and reputation risks.
- The use of a targeted questionnaire during customer due diligence to determine, among other things, whether there is a family member or close associate to whom the PEP rules apply mutatis mutandis.
- PEP check combined with other ongoing screenings, including monitoring for any negative media coverage.

If an existing customer or UBO qualifies as a PEP, the institution will first assess the risk level and then take appropriate measures.

52 FATF (2013), *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)*. It may be useful in this context to be aware of the level of corruption in the country where the person holds the position, for example by referring to Transparency International's Corruption Perceptions Index.
53 It is common for countries to publish lists of names of PEPs as well as lists of positions that are considered to warrant PEP status. See also FATF (2013), *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)*, Chapter 5, under E, "Government-Issued PEP Lists". In addition, the European Commission publishes its own list of PEP positions in EU Member States, and at EU institutions and international organisations.

Good practice: use of red flags

In conducting PEP risk assessments, an institution uses a number of indicators, or red flags. The institution considers the risk higher if, for example:

- the PEP is from a jurisdiction with a higher risk of money laundering and/or corruption, or from an EU- or UN-sanctioned country, particularly if the country in question is an HRTC (see Section 3.3.3);
- there is negative news coverage or case law involving the PEP;
- the information available on the PEP (occupation, age, income) does not match the information on the origin of the funds and assets.
- the information or documents provided on the origin of the PEP's funds or assets:
  - are inconsistent with the information or documents provided by similar customers;
  - originate from high-risk jurisdictions;
  - are inadequate or illogical;
  - are shared through complex, opaque structures (e.g. offshore structures, trusts, bank accounts in high-risk jurisdictions), and the information remains unclear.

Good practice: senior management approval

An institution secures the necessary approval of a senior executive when entering into or continuing a business relationship with, or conducting transactions for, a PEP, according to a predetermined framework (senior management approval framework).

Under this framework, senior management must give prior approval for entering into or continuing a business relationship with a PEP, or for conducting transactions in certain clearly defined low- and medium-risk scenarios appropriate to (i) the size of the institution and (ii) the risks identified in relation to the transaction or business relationship.

Lower management can then assess individual cases to determine whether the business relationship or transaction fits within the predefined framework and whether senior management approval can be assumed. Individual cases that do not fall within the predefined framework must be approved separately by senior management. This approval framework is established and operationalised in accordance with the institution's governance model.

The framework includes the following elements:

- descriptions of the defined risk-based low- and medium-risk scenarios;
- prior approval from senior management for business relationships with, and transactions for, PEPs that fit within the defined scenarios;
- the knowledge and decision-making authority of designated lower management;
- obligation to report PEPs to senior management;
- implementation audit trail.

Designated lower management:

- must have sufficient knowledge of ML/TF risks;
- must have appropriate decision-making authority;
- is adequately informed about the risks of transactions and business relationships with PEPs.

Ultimate responsibility remains with senior management. To demonstrate this, the framework includes an obligation to report to senior management on the institution's position in business relationships and transactions with PEPs. The reporting methodology includes:

- reporting frequency and method, including information on:
  - the number, nature and risk profile of business relationships with PEPs;
  - transactions that lead to an alert are investigated and closed, whether manually or automatically;
- scenarios submitted to senior management for approval;
- monitoring and auditing by second- and third-line parties within the applicable framework.

The compliance function actively monitors and advises on customer acceptance when a PEP is involved.[54] In doing so, it considers the total exposure to PEPs and the actual risk the institution may face if it accepts the customer. Its resources and position allow it to operate and advise independently in these matters. The compliance function's advice on the risk level plays an important role in senior management's decision on the relationship.

Good practice: determining origin of funds and assets for low-risk customers

A domestic PEP enters into a business relationship with an institution, which conducts enhanced customer due diligence. Based on the customer due diligence and product characteristics, the institution classifies the relationship as low-risk. The institution has determined that, in low-risk cases like this, a less intensive investigation into the origin of the funds and assets is sufficient. This means that it assesses the information already available on the origin of the funds and assets and, where justified, requests additional independent data or information.

54 Cf. EBA Guidelines on the role and responsibilities of the AML/CFT compliance officer
55 The European Commission's list is based on the lists published by FATF.

3.3.3 Dealing with high-risk countries (HRTCs)

Legal framework

The *Wwft* stipulates that institutions must conduct enhanced customer due diligence for transactions, business relationships and correspondent banking relationships involving states designated by the European Commission as higher-risk states for money laundering or terrorist financing, also referred to as high-risk third countries or HRTCs. The European Commission identifies countries with strategic weaknesses in their national laws and regulations that pose a significant threat to the EU's financial system. These countries are listed in the annex to Delegated Regulation (EU) 2016/1675.[55]

For transactions, business relationships and correspondent banking relationships involving an HRTC, institutions must take the following additional measures as long as the country is on the HRTC list:

- collect additional information on the customer and UBO;
- collect additional information on the purpose and nature of the business relationship;
- collect information on the origin of the funds used in the business relationship or transaction, and on the origin of the assets of the customer and UBO;
- collect information on the context of, and rationale for, the customer's transaction;
- obtain approval from senior management for entering into or continuing the business relationship;
- apply enhanced monitoring to the customer relationship and transactions by increasing the number of checks, updating the customer and UBO data more frequently and looking for transaction patterns that require further investigation.

When a country is removed from the HRTC list, these additional measures are no longer required.

Institutions must design these measures using a risk-based approach. This means that the intensity of the measures varies with the risk. Institutions must always conduct customer due diligence.

The EBA's ML/TF Risk Factors Guidelines provide further guidance on when transactions, business relationships and correspondent banking relationships are deemed to "involve" an HRTC.

The following laws and regulations are particularly relevant:
- Section 8(1), under b, of the *Wwft*
- Section 9 of the *Wwft*
- Delegated Regulation (EU) 2016/1675

The following other policy statements are particularly relevant:
- EBA ML/TF Risk Factors Guidelines
- FATF: Jurisdictions under Increased Monitoring[56]
- FATF: High-Risk Jurisdictions Subject to a Call for Action[57]

Q&As

Question
Does the *Wwft* require enhanced customer due diligence if the customer is a natural person from an HRTC?

Answer
No, it does not. Barring other circumstances, enhanced customer due diligence is not automatically required if someone is an HRTC national but lives elsewhere. The necessity of enhanced customer due diligence should be determined on a case-by-case basis.

The obligation to conduct enhanced customer due diligence applies if there are transactions, correspondent banking relationships or business relationships involving the HRTC, or if the customer is resident or domiciled in the HRTC. The EBA's ML/TF Risk Factors Guidelines provide further guidance on when this is the case, for example if the funds were generated in an HRTC, transferred from an HRTC or are destined for an HRTC. The above EBA guidelines state that institutions should properly assess the risk associated with the business relationship or transaction if the customer or UBO has close ties with the HRTC. Based on its risk assessment, the institution must determine whether enhanced customer due diligence is required.

Good practice

Good practice: framework for senior management approval

An institution secures senior management approval when entering into business relationships and correspondent banking relationships involving HRTCs using a senior management approval framework. The institution's policy contains a clear and detailed explanation of how to apply this framework (see the good practice "Senior management approval" in Section 3.3.2[58] for more detail).

Good practice: including transactions with HRTCs in the transaction profile

During onboarding, an institution asks about potential transactions involving an HRTC. When the customer indicates that it is going to conduct transactions with suppliers in an HRTC, the institution collects additional information on, among other things, the context of these transactions and considers whether they are appropriate in view of the customer's profile. The institution then conducts a risk analysis on the basis of this information, after which the business relationship is approved by senior management.

56 This list is published on the FATF's website.
57 This list is published on the FATF's website.
58 Note: unlike with PEPs, *transactions* involving HRTCs do not require senior management approval.

The transactions that subsequently take place as part of this business relationship are subject to ongoing enhanced monitoring (transaction monitoring). If transactions are conducted that fall outside the customer's expected transaction profile, these are investigated (see also Section 4.1).

Good practice: contact with customer in case of HRTC-related transactions

For transactions involving an HRTC, an institution decides whether it is necessary to approach the customer for additional information. In some cases, the institution chooses to collect additional information through its own desk research or from public sources, without directly contacting the customer. This is in accordance with the institution's risk-based approach. In its assessment, the institution considers the risk level and its own information position.

For example, after assessing the available information, the institution may come to the conclusion that the customer file contains sufficient information (e.g. on the customer's identity and the origin of the funds) given the nature and risk of the transaction. If this information is up to date, it does not need to be requested again, unless a situation occurs that does not fit the customer's profile.

The institution can also collect certain information (e.g. on the nature of the transaction) by analysing transaction data and/or public sources.

Good practice: changes to HRTC list

An institution monitors changes to the HRTC list. If a country is placed on the HRTC list, the institution takes the additional measures required under the *Wwft* with regard to new and existing customers. For existing customers, it decides whether it is necessary to contact the customer to collect further information based on the information already available and the risk profile. The institution stops applying additional measures to customer files linked to the country once it has been removed from the list.

3.4 Outsourcing customer due diligence

Legal framework

The *Wwft* allows institutions to outsource certain parts of the customer due diligence process to a third party on the basis of an outsourcing or agency agreement. Institutions may have the following components of the customer due diligence process carried out by a third party:

- customer identification and verification of identity (Section 3(2)(a));
- UBO identification and verification of identity (Section 3(2)(b));
- establishing purpose and intended nature of the business relationship (Section 3(2)(c));
- establishing power of representation, identification of representative and verification of identity (Section 3(2)(e));
- investigation of whether a customer is acting on their own behalf, or on behalf of a third party (Section 3(2)(f)).

If the institution outsources its customer due diligence (in its entirety or in part), it remains responsible for compliance with the *Wwft*. If the outsourcing is of a structural nature, the institution must document the arrangement in writing. It is the institution's responsibility to assess whether it is in fact outsourcing these activities.

Outsourcing customer due diligence (in its entirety or in part) under Section 10 of the *Wwft* should be distinguished from the introductory customer screening referred to in Section 5(1)(a) of the *Wwft*. In the case of outsourcing, part of the customer due diligence process is carried out by a third party, which does so on behalf of the outsourcing institution. This third party does not have to be a *Wwft* institution. When a customer is introduced to the institution under Section 5 of the *Wwft*, it can use the results of an investigation carried out by another *Wwft* institution (or, under certain conditions, a branch or majority subsidiary of a *Wwft* institution). For more information about introductory customer due diligence, see Section 3.5.

The following laws and regulations are particularly relevant:
- Section 10 of the *Wwft*

The following other policy statements are particularly relevant:
- EBA guidelines on the role and responsibilities of the AML/CFT compliance officer
- EBA Guidelines on outsourcing arrangements (where applicable)

Q&As

Question
Can an institution outsource the decision on whether to enter into a business relationship with a customer?

Answer
No, an institution cannot outsource the decision on whether to enter into a business relationship with a customer, but the institution can outsource certain elements of the customer due diligence process on which this decision is based.

Question
Which parts of the customer due diligence process is an institution allowed to outsource to a third party?

Answer
An institution may outsource the following elements of the customer due diligence process to a third party:
- customer identification and verification of identity;
- UBO identification and verification of identity;
- establishing power of representation, identification of representative and verification of identity;
- establishing whether a customer is acting on their own behalf, or on behalf of a third party.

Ongoing monitoring cannot be outsourced to a third party.[59]

Question
Is the use of third-party software to support customer due diligence considered outsourcing?

Answer
This can only be determined on a case-by-case basis. In itself, the procurement of standardised software is not generally considered to be outsourcing, as long as the software is implemented solely by the institution. However, if the third-party software provider is more involved in the institution's specific use of the program and adapts the software to the needs of the institution on an ongoing basis, this may qualify as outsourcing. The extent to which customer due diligence is carried out using the third-party software is also a factor in this. It is the institution's responsibility to assess whether its use of third-party software qualifies as outsourcing.

59 Section 3(2)(d) of the *Wwft* (on ongoing monitoring) is not mentioned in Section 10(1) of the *Wwft*. In the case of institutions subject to the Financial Supervision Act (*Wet financieel toezicht – Wft*) where the party effecting the transactions is part of the same group, this party may carry out the ongoing monitoring. Our position on this point, which takes into account current and expected European laws and regulations and the safeguards that apply to outsourcing under the *Wft*, thus remains unchanged.

Good practices

Good practice: outsourcing policy

An institution has properly identified the implications of potential outsourcing and has drawn up a comprehensive general outsourcing policy. The institution regularly reassesses its outsourcing policy, considering whether its outsourcing puts it at risk of inadequate compliance with the *Wwft* and other laws and regulations. The decision to outsource *Wwft* activities is taken by the day-to-day policymakers.

Good practice: risk assessment of outsourcing

An institution seeking to outsource customer due diligence to a third party has assessed the risks associated with this and documented its findings. The risk assessment included an evaluation of the third party's expertise and its compliance with the *Wwft* on behalf of the institution.

Good practice: written agreement

In engaging a third party, an institution has clearly defined its own rights and obligations and those of the third party, setting these out in a written agreement. The agreement covers the following subjects:

- The third party's obligation to comply with the *Wwft* and the institution's policy.
- The accessibility, privacy and security of the personal data involved. For example, the agreement stipulates that the third party must ensure at least the same level of confidentiality and information security with regard to personal data as the institution itself.
- The third party's reporting obligations and the institution's power to audit the third party.
- Termination rights, including the obligation to facilitate the transfer of the outsourced tasks to another third party or the institution itself.

Good practice: monitoring of outsourcing implementation

An institution has maintained sufficient core competencies within its own organisation (e.g. competent compliance functions and auditors) to monitor the implementation of the outsourcing of certain parts of its customer due diligence process. The institution can demonstrate that it can adequately manage and control the service provider and, in extreme cases, take over direct management of the outsourced activity or ensure its transfer to another suitable party.

The institution also regularly evaluates the outsourcing to determine whether the third party still meets the legal requirements and whether the activities are carried out in line with the institution's expectations. The institution periodically tests its processes, systems and use of relevant lists (including the European Commission's HRTC list).

Good practice: outsourcing to service provider outside the EEA

An institution chooses to outsource certain parts of its customer due diligence process to a service provider outside the European Economic Area (EEA). Given the risks that may be involved in this, the institution has paid particular attention to key issues, such as the protection of personal data. It also ensures that it can effectively supervise the party to which the services are outsourced and that the third party acts in accordance with the *Wwft*.

3.5 Introductory customer due diligence

Legal framework

An institution (the accepting institution) may rely on the initial customer due diligence carried out by another institution (the introducing institution). If this is the case, the accepting institution uses introductory customer due diligence and does not need to conduct its own initial customer due diligence. Under the *Wwft*, introductory customer due diligence is subject to a number of conditions:

- the introducing institution must be an institution as referred to in Section 5(1), under a, of the *Wwft*;
- the customer due diligence process must have led to the result required by the *Wwft*; and
- the accepting institution must be in possession of all identification and verification data and other data on the identity of the persons referred to in Section 3(2) to (4) of the *Wwft*.[60]

The required result may also be obtained through a joint effort of the introducing institution and the accepting institution. For example, it may be difficult or undesirable for the introducing institution to establish the purpose and intended nature of the business relationship for the accepting institution. The accepting institution can therefore carry out this part of the initial customer due diligence itself.[61]

In addition, before entering into the business relationship or carrying out a non-recurring transaction, the accepting institution must be in possession of the information and documents used in the introducing institution's customer due diligence. The accepting institution must keep these on file.

The responsibility for carrying out proper customer due diligence and complying with the relevant provisions of the *Wwft*, for example with regard to the documentation of the screening process, remains with the accepting institution at all times.[62]

The following laws and regulations are particularly relevant:

- Section 5(1) of the *Wwft*
- Section 5(2) of the *Wwft*
- Section 5(4) of the *Wwft*
- Section 33(1) of the *Wwft*

Q&As

Question

When a customer is introduced, can the introducing institution's customer's risk profile be copied?

Answer

No, the accepting institution itself is responsible for preparing the risk profile and must do so based on all relevant customer data it is required to have.

60 Parties other than those specified in Section 5(1), under a, of the *Wwft* may be able to perform parts of the customer due diligence process for the institution on an outsourcing basis, as described in Section 10 of the *Wwft*.
61 *Parliamentary Papers II*, 2011-2012, 33 238, no. 3, p. 15.
62 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 51.

Good practices

Good practice: monitoring introducing institutions

In its policy, an institution sets out how it handles its reliance on customer identification and verification performed by introducing institutions, and its relationships with introducing institutions are governed by cooperation agreements. The institution's policy also describes how, when and for what reasons introducing institutions must share customer identification and verification data.

The institution uses a risk-based approach to verify that introducing institutions have adequate customer due diligence processes in place. For example, it may ask institutions that introduce more than 50 customers per year on average to submit their *Wwft* procedures for review. For institutions that introduce more than 100 customers per year on average, an accountant's report on the effectiveness of the *Wwft* procedures may be requested as well. At other institutions, the institution may perform spot checks.

3.6 Ability to enter into a business relationship with a customer or conduct a non-recurring transaction for a customer

Legal framework

Under the *Wwft*, institutions are prohibited from entering into a business relationship with a customer or carrying out transactions for a customer, unless:

- customer due diligence has been carried out in accordance with Section 3 of the *Wwft* (where mandatory);
- initial customer due diligence has led to the required result;
- the institution has all the required identification and verification data, or other relevant data on the identity of the customer, UBO and any representatives.

Institutions are also prohibited from entering into a correspondent relationship with a shell bank[63] or an institution known to allow a shell bank to use its accounts.

In derogation of the obligation to complete customer and UBO verification before entering into a business relationship with a customer, institutions may verify the identity of the customer and UBO during the establishment of the business relationship if this is necessary in order not to disrupt the provision of services, and if the risk of money laundering and terrorist financing is low. In that case, the institution must verify the identity of the customer and UBO as soon as possible after the initial contact with the customer. A bank or financial enterprise may also open an account before it has verified a customer's identity if it ensures that the account cannot be used before verification has been completed.

63 The *Wwft* defines a shell bank as a bank or other financial enterprise as referred to in Section 1a(2) and (3) of the *Wwft*, or an enterprise carrying out activities equivalent to those of a bank or other financial enterprise, which is incorporated in a state where it has no physical presence and which is not part of a supervised group.

If an institution refuses a business relationship or transaction because the customer due diligence did not lead to the required result[64] and there are also indications that the customer in question is involved in money laundering or terrorist financing, the institution is obliged to report this to FIU-NL. In doing so, the institution should also explain why the customer due diligence did not lead to the required result, and why there are indications of money laundering or terrorist financing.

The following laws and regulations are particularly relevant:
- Section 4(3) and (4) of the *Wwft*
- Section 5(1) and (5) of the *Wwft*
- Section 16(4)(a) and (5) of the *Wwft*

The following other policy statements are particularly relevant:
- EBA Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services

Q&As

Question
Is an institution obliged to enter into a business relationship or carry out a non-recurring transaction if the statutory grounds for refusal do not apply?

Answer
No, even if the *Wwft* does not expressly prohibit an institution from entering into a business relationship with, or carrying out a transaction for, a customer, the institution may still decide not to proceed if it concludes that the business relationship or transaction falls outside its risk tolerance. For more information, see also Section 2.1.1.

Question
Should an institution assign a risk profile to each individual customer?

Answer
Yes. An institution must establish a risk profile for each customer based on the information gathered during the initial customer due diligence, including all relevant risk factors. The institution must use the risk profile to assess whether it can enter into a business relationship with, or carry out a non-recurring transaction for, the customer. See also the good practice on the expected transaction profile, as part of the risk profile, in Section 4.1.1.

64 Section 5(1), under b, of the *Wwft* states that customer due diligence must have led to the result referred to in Section 3(2) opening words and subsections a, b, c, e and f, third and fourth paragraphs.

Good practices

Good practice: reporting customer refusal and providing context

An institution receives an application for a business loan to finance rental properties from a company that is not yet a customer. Customer due diligence reveals a number of unusual circumstances. For example, the applicant's property portfolio shows considerable growth in a short period of time. In addition, some of the properties are being sold to the company by private individuals at prices below their property value when they could have fetched a higher price in the regular housing market.

The applicant's answers to the institution's questions are unsatisfactory, which means that the customer due diligence has not led to the required result. The institution also suspects that the applicant may be involved in money laundering and decides not to enter into a business relationship.

Pursuant to Section 16(4) of the *Wwft*, the institution reports the applicant to FIU-NL. In doing so, the institution follows the instructions published by FIU-NL on its website. The report explains the type of financing product involved, why the customer due diligence did not lead to the intended result and that there are suspicions of involvement in money laundering. The circumstances are detailed in the transaction description and the individuals involved are all listed as parties to the report.

Good practice: outside risk tolerance

A potential customer wants to open an account with a bank. The customer is a local bakery, but customer due diligence shows that it is part of a larger structure. The bakery is the only entity within this structure that shows economic activity, and its UBO controls the structure from an HRTC where they are resident. As it is not clear to the bank why the structure has been set up in this way, and given the strong link to an HRTC, the bank determines that the customer structure is outside the risk tolerance defined in its policy.

Good practice: documentation

An institution documents its decision-making process when deciding whether or not to enter into a business relationship or carry out a non-recurring transaction, explaining how it arrived at its decision. The institution also records when it takes the decision, making it possible to verify that customer due diligence was completed prior to entering into the business relationship or that Section 4(3) of the *Wwft* was applied. In documenting this process, the institution follows the EBA's Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services.

Good practice: committee for complex cases

An institution has set up a customer acceptance committee through which senior management decides on acceptance in complex cases. The decision-making process and the decision are consistently documented in the customer file. The follow-up of decisions and any additional mitigation measures are monitored and documented by a designated officer.

4 Customer due diligence: ongoing monitoring

The *Wwft* requires institutions to monitor their business relationships and the transactions conducted over the course of those relationships on an ongoing basis. As part of this ongoing monitoring, institutions monitor their customers' proposed and completed transactions in order to detect unusual transactions (see Section 4.1).

This chapter discusses the following elements of transaction monitoring:

- business rules and models (see Section 4.1.1);
- pre-transaction monitoring (see Section 4.1.2);
- post-transaction monitoring (see Section 4.1.3);
- alert handling (see Section 4.1.4);
- feedback and testing (see Section 4.1.5);

Institutions are obliged to report unusual transactions to FIU-NL (see Section 4.2). In addition, the *Wwft* stipulates that institutions must repeat the customer due diligence process in certain circumstances, and that they must take reasonable measures to keep customer information up to date (see Section 4.3). A customer review may lead an institution to adjust the customer's risk profile. In certain cases, an institution may decide to terminate a business relationship with a customer on the basis of its monitoring (see Section 4.4).

4.1 Transaction monitoring

Legal framework

As part of customer due diligence, the *Wwft* requires institutions to carry out ongoing monitoring of their business relationships and the transactions carried out over the course of these business relationships to ensure that they match what the institution knows about the customer and the customer's risk profile. In addition, the *Wwft* requires institutions to use the indicators listed in the *Wwft* Implementation Decree to assess whether a proposed or completed transaction is unusual and, if so, whether it should be reported to FIU-NL (see Section 4.2). To meet these obligations, institutions must monitor their customers' proposed and completed transactions.

A transaction is an act or a combination of acts performed by or on behalf of a customer of which the institution has taken note in the provision of its services to that customer. This definition includes payment transactions, pledge orders, redemption requests, bank account changes and cash deposits. In short, it includes all transactions related to the institution's services. A payment from an institution itself to one of its own suppliers, for example, falls outside the scope. The words "act or a combination of acts performed by or on behalf of a customer" should be interpreted in such a way that the passive involvement of the institution (by virtue of its knowledge of the transaction) falls under the statutory obligation to report unusual transactions. With this broad definition of the term transaction, the legislator intended to make it clear that the obligation to report unusual transactions applies not only to the transactions carried out by institutions themselves, but also to those they encounter in the course of providing their services. This prevents institutions from providing services that help perpetuate money laundering or terrorist financing.[65]

The EBA's ML/TF Risk Factors Guidelines provide further guidance on how to conduct transaction monitoring, including with regard to how institutions can tailor the frequency and intensity of their transaction monitoring to the customer's risk profile.

Institutions must pay particular attention to unusual transaction patterns and transactions that, due to their nature, typically carry a higher risk of money laundering or terrorist financing. In any case, the *Wwft* prescribes enhanced monitoring for transactions involving PEPs or HRTCs, complex or unusually large transactions, transactions with an unusual pattern or without a clear economic or lawful purpose (see Section 3.3).

The following laws and regulations are particularly relevant:

- Section 1(1) of the *Wwft*
- Section 2a(1) of the *Wwft*
- Section 3(2), under d, of the *Wwft*
- Section 8(3) and (5), under b, of the *Wwft*
- Section 9(1) of the *Wwft*
- Section 15(1) of the *Wwft*
- Section 16(1) of the *Wwft*
- Section 4 in conjunction with Annex 1 to the *Wwft* Implementation Decree

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- EBA Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services

65 *Parliamentary Papers II*, 33 238, no. 3.

Rationale

An institution that adequately monitors its customers' proposed and completed transactions can take timely action if there is reason to believe that a transaction, or a pattern of transactions, may be related to money laundering or terrorist financing.

Good practices

Good practice: automated transaction monitoring

An institution decides to automate its transaction monitoring based on the risks involved and the nature and size of the transactions. It takes this decision to ensure effective, consistent and rapid monitoring, and to meet its ongoing monitoring obligations.

The institution begins by identifying all source systems that contain relevant transaction data to ensure that all required data on customers, services and transactions is fully and accurately included in the transaction monitoring process. It also creates detailed business rules that identify suspicious transactions based on predetermined criteria, such as transactions above a certain amount or transactions to high-risk regions.

In addition, the institution develops sophisticated models based on historical data and behavioural patterns to predict suspicious activity, which it integrates into its automated transaction monitoring system to identify suspicious transactions more accurately.
To ensure the effectiveness of the automated system, the institution conducts regular tests. It can use historical data to check that all suspicious transactions have been correctly identified and that there are no unintended side-effects, such as discrimination. Based on the results of these tests, the institution adjusts and tweaks its business rules and models as necessary to improve the accuracy and effectiveness of its transaction monitoring.

Good practice: dynamic transaction monitoring

An institution ensures that its transaction monitoring is dynamic, closely monitoring the mitigated risks from its company-wide risk assessment. This dynamic process comprises three main elements:

- Business rules and risk-based models (see Section 4.1.1):
  The institution bases its business rules and models, including the associated threshold values, on the nature and magnitude of the identified risks. This includes rules on cash transactions and transactions to high-risk countries.
- Tests (see Section 4.1.5): The institution conducts regular testing, verifying that the identified risks are adequately detected by the transaction monitoring system. These tests use historical transaction data to assess whether the system is effective in identifying transactions related to the identified risks. The insights from these tests are implemented in the institution's operational management.
- Documentation: If the tests lead to any conclusions or adjustments, these are documented along with the decision-making process.

If the tests show that a certain risk is not yet adequately detected, the institution may introduce additional mitigation measures. This approach ensures that the transaction monitoring system is continuously aligned with the institution's current risk profiles, contributing to effective and dynamic risk-based transaction monitoring.

4.1.1 Business rules and models

Rationale

The risk assessment is the foundation for transaction monitoring. If an institution is aware of how it could become involved in money laundering or terrorist financing and applies this knowledge (as well as other risk knowledge) to transaction data, the probability of detecting relevant transactions increases. An institution can apply its risk knowledge through business rules. It can also leverage this knowledge by using advanced models, for instance based on machine learning (ML) software, instead of traditional business rules. This allows institutions to identify complex patterns and anomalies that may indicate suspicious activity.

Q&As

Vraag

Should an institution systematically review its business rules and models?

Antwoord

Yes, an institution must put in place a process to systematically monitor and assess the effectiveness of the business rules and models it uses, and make adjustments where necessary.

Good practices

Good practice: knowledge and typologies

An institution uses its knowledge about customers and typologies that may indicate money laundering or terrorist financing to effectively monitor transactions. The institution incorporates this knowledge in:

- Business rules to detect potential money laundering and terrorist financing patterns, for instance in the form of scenarios and associated transaction limits.
- Models, such as models that can identify customers who exhibit unusual behaviour compared to their reference group, models that perform network analyses, or models that can distil transactions with similar characteristics from transaction data based on historical reports of unusual transactions.
- A handbook or work instructions for manual transaction monitoring.

Good practice: linking business rules and risk assessment

An institution has established a number of business rules based on its risk assessment. It has also documented the link between its risk assessment and the business rules.

In creating the business rules, the institution considered a number of factors, including:

- the type of customer (e.g. private individual, business customer, PEP);
- the customer segment;
- the customer's risk profile, as drawn up during customer acceptance and adjusted later where necessary (e.g. low, medium or high);
- the transaction's country of origin or country of destination, (e.g. international transactions between two offshore countries that are routed through the Netherlands);
- the product (e.g. savings, property finance or trade finance);

- the distribution channels (e.g. physical or online presence of the customer);
- the nature and frequency of the transactions (e.g. cash or non-cash);

The institution also used comparisons with the customer's other transactions and with the customer's peer group in creating the business rules.

Good practice: design of business rules

An institution has substantiated the choices it made in designing its business rules, and it can demonstrate their adequacy. The institution has:

- clearly defined the threshold values;
- ensured that the business rules include various threshold values for high-risk customers in the context of enhanced monitoring;
- ensured that the business rules include various threshold values for different products or services.

Good practice: reference groups in transaction monitoring

An institution has classified its customers into reference groups, which it uses to assign individual risk profiles and expected transaction profiles. The institution also uses these reference groups to identify customers who exhibit anomalous transaction behaviour compared to their peers. Institutions can define these reference groups themselves, but they should be sufficiently homogeneous. Reference groups can be defined on the basis of a number of customer characteristics, such as sector, legal form, age, natural personhood, transaction behaviour, income, country of origin, etc. The institution sets its threshold values for transaction monitoring based on the usual behaviour of customers within a reference group. For example, the threshold values used to monitor minors will be different from those used for small business.

Good practice: expected transaction profile

An institution uses expected transaction profiles for its customers in cases where this can help it detect unusual transactions. An expected transaction profile provides insight into the customer's expected transactions and the associated business rules. By identifying a customer's expected transaction behaviour, the institution can assess whether the transactions carried out are consistent with what they know about the customer. This means that an expected transaction profile is only useful if it is sufficiently distinctive and applied to an individual customer or a sufficiently homogeneous group of customers.

The institution has therefore included lower threshold values in the expected transaction profile for its underage customers compared to the transaction profiles for older customers, and it also takes into account income and other distinguishing characteristics.

The institution may, if appropriate to its customer base, establish expected transaction profiles using reference groups (or peer groups). It can also collectively assign an expected transaction pattern to customers that belong to a reference group, which means that it does not need to conduct further investigation into expected transactions prior to transaction monitoring. The institution must conduct ongoing monitoring to assess whether the expected transaction profile is still appropriate or needs to be adjusted.

The institution uses the expected transaction profile to check whether the transactions carried out over the course of the business relationship match what it knows about the customer. If the customer's transactions deviate from the expected transaction profile, the institution adjusts the expected transaction profile. In addition, the institution assesses whether it needs to adjust the frequency and intensity of its transaction monitoring.

Good practice: enhanced monitoring of PEPs and HRTCs

In its policy, an institution has set out how it handles the required enhanced monitoring of PEPs and HRTCs. The institution does this as follows:

- Risk assessment: The institution conducts a risk assessment to identify the specific risks associated with PEPs and HRTCs. This includes an analysis of the relevance of factors such as political positions, spheres of influence and the reputation of PEPs, as well as the risk profiles of countries that are considered HRTCs in relation to its portfolio.
- Adjusting measures: Based on the risk assessment, the institution adjusts its measures to ensure proper enhanced monitoring of PEPs and HRTCs. This includes improving its customer identification procedures, conducting more extensive customer due diligence and implementing specific monitoring mechanisms for transactions involving PEPs and HRTCs.
- Ongoing monitoring and adjustment: The institution conducts ongoing monitoring of its customer base and transactions involving PEPs and HRTCs. New risks and developments are closely monitored and adjustments are made where necessary.
- Training and awareness: Employees receive regular training and are kept informed about the risks associated with PEPs and HRTCs, as well as the specific measures that must be applied. This raises awareness within the institution and ensures that employees are equipped to deal with these specific risks.

Good practice: use of artificial intelligence/machine learning models

An institution implements an AI/ML model in its transaction monitoring process. The model identifies transactions that match known risk patterns, but it also has the capacity to detect new and lesser-known risks. It does this, for example, by identifying transactions that deviate significantly from established behaviour patterns. This process involves training the system to teach it what is considered "normal", after which it can flag anomalies that may be indicative of money laundering or terrorist financing. In implementing the model, the institution has ensured that several crucial preconditions are met. These include:

Soundness: The institution ensures that the ML model is based on sound methodologies and validated data. This includes the use of high-quality data, robust algorithms and regular reviews to ensure the model's accuracy and effectiveness.

Accountability: The institution defines clear responsibilities for the design, implementation and maintenance of the ML model. Procedures are established to track the model's decisions and outcomes, and to ensure that the institution is able to explain the actions taken.

Fairness: The ML model is developed with a focus on fairness and equality. Measures are taken to prevent or reduce bias and discrimination, for example by carefully selecting features, conducting bias analyses and applying fairness checks.

Ethics: The institution adheres to ethical guidelines and standards when using the ML model, respecting customers' privacy, protecting their rights and avoiding unintended negative consequences for individuals or communities.

Skills: The institution ensures that the team responsible for developing, implementing and managing the ML model has sufficient skills and expertise. It does so, for instance, by offering training and development opportunities to guarantee a deep understanding of ML techniques, including with regard to identifying and addressing biases and discrimination.

Transparency: The institution promotes transparency through clear communication on the use and operation of the ML model. It provides clear documentation and explanations of the algorithms used, the decision-making processes, the potential risks of biases and discrimination, and the measures taken to mitigate these risks.

Good practice: risk tolerance and business rules

An institution has determined its risk tolerance and translated this into business rules and/or models, defining appropriate threshold values for the number of payment requests, crypto payments, payments to and from high-risk countries, and cash withdrawals and deposits, as well as for other transactions. This means that transactions that exceed these threshold values are flagged by the transaction monitoring system, after which they are investigated.

Good practice: threshold values

An institution has established transaction monitoring rules based on its risk assessment and risk tolerance. For SMEs, transactions below a certain threshold value may or may not generate an alert, depending on other relevant factors. In determining this threshold value, the nature of the business and the applicable objective transaction reporting indicators are taken into account.

Besides the business rules, the institution also uses a machine learning model to detect anomalous transactions. By analysing historical transaction data and customer information, the model can identify patterns and anomalies indicating unusual transactions. For customers who make an individual transaction below a threshold value set by the institution, an alert may or may not be generated, depending on other relevant factors. If an alert is generated, the institution assesses whether it needs to discuss this with the customer.

With regard to the cash risk factor, the institution's business rules and models only generate an alert for transactions above a certain threshold value and transactions below this threshold value do not generate an alert. The threshold values are based on common transaction volumes in the relevant customer sector and the applicable objective indicators for reporting cash transactions. When an alert is generated, the institution also considers other risk factors before deciding whether it is necessary to contact the customer.

Good practice: high-risk jurisdictions

An institution's transaction monitoring system pays extra attention to high-risk jurisdictions. Its business rules and/or models include components based on which alerts are generated with respect to these countries. To identify high-risk jurisdictions, the institution uses several sources:

- The European Commission's list of high-risk countries.
- The FATF warning lists.
- Transparency International's Corruption Perceptions Index.
- An internal list maintained based on in-house analysis, incidents, FIU-NL reports and international money laundering scandals.

4.1.2 Pre-transaction monitoring

Rationale
Pre-transaction monitoring allows institutions to detect, reject and report unusual transactions, as well as other transactions that fall outside their risk tolerance, before or during the execution of the transaction. In deciding to refuse a transaction, institutions also take into account the fact that assisting in a criminal offence, such as money laundering, is prohibited.

Good practices

Good practice: pre-transaction monitoring process

An institution has an automated process in place to detect and, if necessary, stop potentially unusual transactions. Employees use specific guidelines to assess whether a proposed transaction qualifies as unusual. First- and second-line employees were involved in drafting these guidelines, and the institution's risk profile was taken into account.

The process ensures that proposed transactions flagged as unusual by the first line are referred to the compliance function for review. If it is determined that the proposed transactions are in fact unusual, they are reported and, if necessary, refused.

Good practice: transaction patterns

An institution uses data analysis to detect transaction patterns as well as networks and combinations of transactions conducted by one or more customers that may indicate money laundering or terrorist financing at an aggregate level. This involves:

- The use of advanced analytical techniques: the institution uses advanced analytical techniques to examine transaction data and identify patterns that may indicate suspicious activity. It uses statistical analysis, network analysis and other data analysis techniques to understand the relationships and patterns within transaction data.
- Data aggregation and integration: the institution has explored how it can aggregate and integrate transaction data from different sources to get a complete picture of the transaction landscape. This may also include combining internal transaction data with external data sources and open-source intelligence (OSINT) to gain a full overview of the potential risks.
- Real-time monitoring: the institution implements real-time monitoring of transaction patterns and networks, ensuring a rapid response to suspicious activity. This includes the use of automated systems that generate alerts for potentially risky transactions.

Good practice: analytical tools

An institution uses analytical tools to detect unusual transactions and/or unusual transaction patterns based on insights from the literature or outlier detection. It uses these analytical tools alongside its post-transaction monitoring system. These ad hoc analyses enable the institution to determine the extent to which its services are vulnerable to financial crime, the extent to which it occurs in the institution and how it can be detected. This allows the institution to keep adapting to new forms of financial crime.

Good practice: refusing a transaction after pre-transaction monitoring and the tipping off prohibition in relation to reporting

During pre-transaction monitoring, an institution detects a proposed transaction with a significant risk of money laundering or terrorist financing. The institution therefore refuses the transaction and reports it to FIU-NL. It does not inform the customer of the unusual transaction report submitted to FIU-NL.

Good practice: growing transaction amounts, refusing services

A money transaction office notices that one of its customers regularly transfers money to the same individual in a third country. In two months, the total amount transferred is over €10,000. After a brief investigation, the institution concludes that there is no logical explanation for these transactions. The transactions that have already been carried out are reported to FIU-NL. When the customer tries to make another transaction, they are unable to provide an adequate explanation regarding the origin of the funds when asked. The institution refuses the transaction and reports it to FIU-NL.

Good practice: life insurer refuses policy surrender

A customer takes out an accumulation policy from a life insurer. Through an intermediary, the customer deposits €750,000. Four months later, the customer wants to terminate the policy, entitling them to a surrender charge from the insurer.

The insurer suspects money laundering and refuses to pay the surrender charge. The deposit and intended surrender are reported to FIU-NL.

Good practice: suspected money laundering transaction

A bank is involved in the sale of property owned by a customer. A party from a jurisdiction that has a reputation as a safe haven for criminal funds shows interest in the property. When the bank inquires about the origin of the funds, the interested party indicates that the money is being made available by a party based in the Middle East that acquired its assets through oil extraction in South America. The party provides a bank statement from an Asian company owned by the Middle Eastern party as proof.

The bank's research shows that the South American oil fields referred to by the interested party have very low yields. Further investigation reveals that the Asian bank does not recognise the bank statement provided.

The bank refuses the transaction and files a report with FIU-NL.

Good practice: products do not match customer profile

When a customer applies for documentary credit with a bank, the bank notices that the products involved do not fit the customer's business model. The transaction is put on hold and reported to the compliance function, which recommends making inquiries with the customer. Inquiries by the account manager subsequently reveal that the customer has started a second business activity and is making investments to facilitate this. The customer provides evidence of this. The compliance function approves the transaction, after which it is executed. The account manager updates the customer file.

4.1.3 Post-event transaction monitoring

Rationale

Post-event transaction monitoring involves monitoring transactions after they have been executed. This allows institutions to identify transactions and transaction patterns that indicate possible involvement in money laundering or terrorist financing.

Good practices

Good practice: various alert generation methods

An institution has various detection methods that can generate alerts:

- Part of the monitoring can be conducted using business rules, allowing the institution to identify and investigate transactions that match an objective indicator, as well as deviations from the expected transaction profile. Moreover, the use of business rules allows the institution to check whether typologies that are relevant given its risk profile occur in its transactions.
- Another part of the monitoring can be conducted using AI and models. This allows the institution to better detect and investigate potential unusual patterns and complex transactions.
- An institution uses data analysis and modelling to detect unusual figures ("outliers"). In doing so, it can consider transaction volumes, numbers of transactions, transactions to high-risk countries or sectors, and anomalous patterns in IP address data or other technical characteristics.

Good practice: terrorist financing alert generation

An institution notices a debit card transaction carried out by a customer based in an area near the border of a country at war. This country is also associated with terrorism. The institution checks the transaction against a list of towns and cities in the border area published by FIU-NL as part of its news reports. The monitoring system generates a terrorist financing alert for the transaction. The institution conducts further investigations based on the alert.

Good practice: indicators for use of cash

In its policy, an institution has identified indicators for when a customer's use of cash requires further attention. These indicators show that the institution is mindful of:

- what it sees as withdrawals or deposits of unusual amounts by a customer in a specific sector.
- what it sees as unusual withdrawal or deposit patterns.
- withdrawals or deposits of an unusual number of large denominations (e.g. €200 and €500 notes) where this cannot be explained by the customer's business activities. Increased vigilance is particularly warranted if a customer uses €500 notes.
- frequent transactions that may indicate "smurfing" (splitting large transactions into several smaller ones with the aim of staying below any cash limits or reporting limits).

In this context, the institution also pays attention to the obligation to report to FIU-NL (see Section 4.2). A single transaction involving a few high-denomination notes does not in itself warrant further attention, unless it is inconsistent with the information the institution has gathered about the customer, in which case the institution conducts an investigation.

4.1.4 Alert handling

Rationale

An alert is a signal indicating a potentially unusual transaction. This includes transactions that fall outside the expected pattern and/or profile, as well as transactions that do not appear to have an economic or legal purpose. Alert handling is important to ensure that unusual transactions are spotted and reported to FIU-NL without delay.

Good practices

Good practice: alert handling process

Institutions must have procedures and working processes in place to assess and handle alerts. Relevant staff must receive up-to-date instructions and training to recognise unusual transactions.

The procedures and working processes state that every alert must be assessed using a risk-based approach and, if necessary, investigated. If there is an alert (or a combination of alerts), the institution must determine whether an unusual transaction has taken place using customer and transaction data. Where necessary, external sources must be consulted, and/or the customer must be asked about the context and purpose of the transaction. The assessment of an alert may lead to a reassessment of the customer's risk profile.

These procedures and working processes must ensure that the processing time from the moment an alert is generated to the moment a report is filed with FIU-NL is as short as possible, and that the right priorities are set when dealing with alerts. One such priority is that proposed or completed unusual transactions must be reported to FIU-NL immediately after the unusual nature of the transaction becomes known.

The institution has reliable management information regarding its working process for alert handling, and this information includes relevant data points, such as the processing times for alert handling.

The institution also documents its considerations and conclusions with regard to closing an alert or reporting the transaction as unusual to FIU-NL.

Good practice: responsibilities with regard to alerts

The organisation is structured such that the first line has primary responsibility for transaction monitoring, and that the compliance function (if the institution has one) oversees the process and advises. The compliance function is also responsible for reporting unusual transactions to FIU-NL. It is therefore important that the institution has a procedure in place that ensures the compliance function's involvement if an unusual transaction is detected.

Good practice: automated alert closing

An institution has a process in place to automatically close alerts for low-risk transactions. In this context, the institution has:

- taken pre-emptive measures appropriate to its risk tolerance in relation to certain transactions;
- thoroughly documented the underlying risk-based decision model;
- set up a procedure in which automatically closed alerts are evaluated, for instance using random checks. The institution is also aware of the fact that a relatively large number of automatically closed alerts may indicate an inadequate decision model.

Good practice: tourist spending

A customer is on holiday in an HRTC and spends money there on tourist activities. As a result of heightened scrutiny of transactions related to HRTCs, the institution takes note of the alerts this generates. It analyses the transactions, using the transaction information as additional information, and determines that the customer is spending money on tourist activities. Taking into account the customer's expected transaction profile, the institution therefore concludes that there is a low risk of money laundering and terrorist financing. The institution has sufficient information and sees no reason to contact the customer. The conclusion is documented and the alerts are closed.

Good practice: alert analysis

An institution's transaction monitoring system generates an alert following substantial cash deposits into a business account. The institution conducts an analysis of the customer and transaction profile, which establishes that the account is held by a hospitality establishment and that the customer file does not list any specific risks. An additional background investigation into the customer reveals a transparent situation and no record of any past issues.

The transaction analysis shows that frequent cash deposits are made into the account, with a monthly volume fluctuating between €5,000 and €15,000. One summer month, the customer deposited more than €20,000, exceeding the expected volume of cash deposits in their risk profile. The analysis shows that the customer's cash deposits amount to a stable percentage of their total income.
Based on the institution's work instructions, the alert handler is able to confirm that this percentage is in line with the applicable ratios for this sector. The customer's cash deposits can thus be explained by their regular business activities, which commonly show a seasonal pattern and a higher income during the summer period.

Based on the analysis, the alert handler concludes that the cash deposits are not unusual. This conclusion is documented and no report is filed with FIU-NL.

Good practice: terrorist financing alert analysis

A customer withdraws cash in a region that has frequently been in the news because a terrorist organisation has been active in a neighbouring country, where it is trying to recruit new members. People from different countries have been travelling to this region to cross the border and join the terrorist organisation. The bank has therefore identified the region as a high-risk area. As a result, the customer's cash withdrawal triggers an alert, but the institution concludes that it does not qualify as an unusual transaction. The amount involved is small, and there are no further indications of money laundering or terrorist financing. This decision is documented.

Two months after this transaction, the customer applies for a €10,000 loan from the bank. A bank employee finds that this customer already applied for a €10,000 loan four months earlier. At the time, the customer stated that the loan – which was granted – would be used to purchase a car, among other things. This combination of circumstances prompts the employee to conduct further investigations, which reveal that the amount of the first loan was almost immediately transferred abroad in several transactions. The employee also suspects a connection with the previous alert, for the debit card transaction in the high-risk area.

Based on these findings, the employee asks the customer several questions about the financial flows in relation to the loan intended for the purchase of a car, but the customer is unable to provide a clear explanation for the transactions. The bank decides to refuse the second loan and reports all transactions – the debit card transaction and the two loan applications – as unusual transactions to FIU-NL.

4.1.5 Feedback and testing

Legal framework
Pursuant to Section 2c(4) of the *Wwft*, institutions are obliged to systematically review their guidelines, procedures and measures (including their transaction monitoring system) and ensure that these are adjusted where necessary (see also Section 2.1.2).

Rationale
As new risks arise and old risks cease to be relevant, an institution's risk assessment changes, which could mean that the transaction monitoring system needs to be adjusted as well. In addition, models or business rules may prove ineffective in practice: they may not generate enough relevant alerts, or they may generate too many irrelevant ones. Ongoing testing and fine-tuning of the transaction monitoring system helps increase its effectiveness.

Q&As

Question
Is testing still required if advanced transaction monitoring techniques are used?

Answer
Yes, with advanced techniques it is especially important to validate results so that unexpected and potentially undesirable outcomes are identified in time. Backtesting and comparison with other detection techniques can play an important role in this.

With self-learning systems, it is important to ensure that developments in the model do not gradually lead to non-plausible or undesirable results.

Good practices

Good practice: testing transaction monitoring system

An institution documents how it arrived at the definitions of its business rules, what it does to maintain them on an ongoing basis and how it periodically tests them, for example through the use of backtesting. The institution uses the results of the backtests to assess the effectiveness of the applied business rules and models, and makes adjustments where necessary.

The institution also uses management information to monitor whether the output of the various business rules and models (e.g. numbers of alerts, FIU-NL reports and corresponding amounts) matches the risks identified in the risk assessment. This is called coverage testing. If the transaction monitoring system's output is too limited, this helps the institution understand which business rules and models do not adequately cover the inherent risks in the portfolio. It also helps the institution determine whether additional measures need to be taken.

The institution documents the results of these analyses as well as the analysis process and any relevant considerations. The structural design of the quality assurance process and the periodic tests is also documented. Where necessary, the institution makes adjustments based on the results of the tests.

The institution also uses lessons learned from FIU-NL reports, incidents, thematic investigations and customer reviews to assess whether the risk assessment is still up to date, and whether the transaction monitoring system needs to be recalibrated.

Good practice: feedback loop

An institution has a system in place that regularly evaluates the effectiveness of its business rules and models. The system analyses a wide range of variables to determine which variables could potentially improve the performance of the business rules and models.

A periodic review has identified a business rule for international transactions with many more false positives for transactions within the EU than for transactions outside the EU.

The institution has supplemented this observation with a data analysis and risk assessment to verify whether the envisaged risk is still fully covered by the business rule in the event of potential adjustments. The institution then adjusts the business rule by raising the threshold value for transactions within the EU compared to that for transactions outside the EU. The feedback loop has thus resulted in a more effective business rule.

Good practice: using FIU-NL data and typologies

An institution has a procedure in place to ensure that its risk assessment is updated based on input from FIU-NL reports and FIU-NL feedback. The institution also recognises that risks and perceptions change, which may mean that issues that would have been reported in the past can now be ignored. Other sources, such as typologies and recent developments, are used to recalibrate the risk assessment as well. Based on the updated risk assessment, the institution also reviews its working methods, business rules and models, and adjusts these where necessary.

Good practice: identifying false negatives

Following a publication about a money laundering case, a bank checks payments made to the country involved. It finds that several of its customers have made large numbers of transactions to this country in a short period of time.

The bank notes that its transaction monitoring system did not generate alerts for these transactions. Concluding that this is undesirable, it adjusts its business rules or models to ensure that these kinds of transactions do generate alerts in future. In addition, the bank assesses whether the transactions should be reported to FIU-NL.

Good practice: backtesting

Business rules and models can be evaluated using backtesting. Backtesting uses historical data, such as transactions and reported transactions, to test the accuracy of a business rule or model. Based on the results of this, an institution can make necessary adjustments to the transaction monitoring system.

The aim of these tests is to further optimise the business rules and models and make them more effective in order to generate more true positive alerts and reduce the number of false positives.

There are different kinds of backtesting, including:

- Retrospective analysis of a selection of transactions that under a previous system configuration did not generate an alert. The aim of this is to assess whether the transaction monitoring system was right not to produce an alert for these transactions (a true negative) or whether certain transactions are in fact indicative of unusual behaviour (a false negative).

- An analysis of transactions that have been identified as possibly unusual through a method other than post-event transaction monitoring. The aim of this type of backtesting is to analyse the extent to which the transaction monitoring system is able to detect unusual transaction patterns and transactions.
- An analysis of business rules that only, or mostly, generate false positive alerts. The aim of this test is to review whether these business rules are relevant and how they might be adjusted to generate more true positives.
- A test that analyses whether the system enables the institution to comply with the obligation to report unusual transactions without delay.

4.2 Reporting unusual transactions

Legal framework

Reporting obligation

Pursuant to the *Wwft*, an institution has the duty of reporting to FIU-NL of executed or proposed unusual transactions immediately after their unusual nature has become known. The *Wwft* Implementation Decree sets out indicators for each type of institution, which must be used to assess whether a transaction qualifies as unusual. Most of these indicators are objective. Objective indicators generally include an objective threshold amount that determines when a transaction must be reported to FIU-NL. A transaction must also be considered unusual if the institution has reason to believe that it may be related to money laundering or terrorist financing on the basis of a subjective indicator. The *Wwft* Implementation Decree also stipulates that if transactions are reported to the police or the Public Prosecution Service in connection with suspected money laundering or terrorist financing, it is appropriate that they are also reported to FIU-NL, given the assumption that these transactions may be related to money laundering or terrorist financing.

Pursuant to the *Wwft*, an institution's compliance function (if it has one) is responsible for reporting unusual transactions.

Institutions must provide a number of details when filing a report. These include:

- the identity of the customer, the identity of the UBOs and, to the extent possible, the identity of the party on whose behalf the transaction is effected;
- the type of identity document presented by the customer and the number of the identity document (where applicable, this also applies to the other persons referred to under a);
- the nature, time and place of the transaction;
- the value, origin and destination of the funds or other assets involved in the transaction;
- the circumstances based on which the transaction has been earmarked as unusual;

FIU-NL may share information on institutions' reporting behaviour with DNB.

FIU-NL information request

FIU-NL may request data or intelligence from an institution that has submitted a report, or from an institution that it believes has data or intelligence relevant to its analysis of an executed or proposed transaction or business relationship. The institution must provide such data or intelligence to FIU-NL without delay.

Indemnification

The *Wwft* includes a criminal-law indemnity in relation to the reporting obligation. This ensures that data or information provided by an institution that reports an unusual transaction in good faith (either on its own initiative or in response to an FIU-NL information request) cannot be used in a criminal investigation or prosecution of that institution on suspicion of money laundering or terrorist financing. This indemnity applies to persons working for the institution as well.

The *Wwft* also includes a civil-law indemnity, which means that an institution cannot be held liable under civil law for any loss suffered by a third party (including the customer) as a result of a report, as long as the institution acted on the reasonable assumption that it was fulfilling its reporting obligation.

Tipping off prohibition

Institutions, and the persons working for them, may not disclose to anyone that an unusual transaction has been reported (the tipping off prohibition), as this could obstruct the investigation.

The *Wwft* contains some exceptions to the tipping off prohibition. For example, two institutions belonging to the same group may, under strict conditions, exchange information on a report. The same applies to two institutions that have a common customer and are involved in the same transaction.

The following laws and regulations are particularly relevant:

- Section 15 of the *Wwft*
- Section 16(1) and (2) of the *Wwft*
- Section 17 of the *Wwft*
- Section 19 of the *Wwft*
- Section 20 of the *Wwft*
- Section 23 of the *Wwft*
- Section 23a of the *Wwft*
- *Wwft* Implementation Decree

The following policy statements are particularly relevant:

- General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act, issued by the Ministry of Finance and the Ministry of Justice and Security
- FIU-NL instructions
- EBA Guidelines on the role and responsibilities of the AML/CFT compliance officer

Rationale

When institutions report unusual transactions to FIU-NL, authorities are better able to deploy targeted investigative tools to counter money laundering and terrorist financing.

Q&As

Question

Should institutions continue to report to FIU-NL if they also receive a requisition regarding a customer or transaction from the Public Prosecution Service?

Answer

Yes. Institutions may receive a requisition from the Public Prosecution Service as part of a criminal investigation. If this is the case, the obligation to report unusual transactions remains, even if the transactions are related to the requisition.

Question

Should institutions continue to report to FIU-NL if they have also reported a criminal offence to the police?

Answer

Yes. FIU-NL investigates reported transactions. This may result in a transaction being declared suspicious, in which case FIU-NL reports the transaction to the investigative authorities. The investigative authorities can then use this information to detect and investigate crimes.

Good practices

Good practice: reporting by institutions that have no compliance function

An institution that does not have a compliance function has defined in its policy who is responsible for reporting unusual transactions. In designing its policy, the institution has taken into account the EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer. The institution ensures that the person responsible for implementing the reporting process has sufficient powers, capacity and resources to do so. This also means that other (first-line) priorities must not impede or affect the reporting process. The decision to report must be made independently. If the first line is responsible for the implementation of the reporting process (in its entirety or in part), the employees involved must be able to perform this part of their work independently, and independently of their first-line work.

Good practice: outsourcing

An institution has outsourced its compliance function, including the task of reporting unusual transactions to FIU-NL. In doing so, the institution has taken into account the EBA's Guidelines on the role and responsibilities of the AML/CFT compliance officer. The institution itself determines whether a transaction is unusual, which is the responsibility of the first line.

Good practice: reporting procedure

An institution reports proposed or executed unusual transactions to FIU-NL, fully and without delay. It does so in accordance with FIU-NL's reporting instructions. The institution has policy in place that sets out the internal reporting process and what steps to take in case an unusual transaction is detected. The policy also ensures that a report is filed without delay, as soon as the unusual nature of a transaction becomes known.

As part of the policy, the customer's previous and related transactions are included in the investigation to assess whether there are any other unusual transactions that should be reported. The customer's risk profile and the corresponding transaction profile are reassessed as well. The policy also stipulates that the institution documents its decision-making process if it decides not to report a transaction.

Good practice: training programme

An institution provides sufficient guidance to its staff on the reporting of unusual transactions, for example by discussing case studies (taken from practice) on a quarterly basis and including them in the regular training programme.

Good practice: reporting based on objective indicator

An institution has set up an automated reporting process for transactions that match an objective indicator. The compliance function periodically reviews the effectiveness of this process, assessing its completeness and accuracy. The process prevents the institution from potentially failing to report unusual transactions without delay and reduces the administrative burden.

Good practice: confidentiality and tipping off prohibition

An institution has laid down in its policy how it ensures confidentiality regarding unusual transactions and reports to FIU-NL under the tipping off prohibition. This also includes periodically providing information and training to relevant staff, including employees who interact with customers. It is essential that these employees are able to identify potentially unusual transactions, and that they know what questions they have to ask the customer and what information they must not disclose to the customer.

The policy also pays attention to securing information flows and assigning appropriate access rights to the recorded information used to handle alert reports of potentially unusual transactions.

Good practice: threshold amounts

Where objective indicators are related to a specific transaction limit, the institution also assesses 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 the institution suspects a connection and the transactions collectively exceed the threshold amount, the institution reports these transactions as a subjective indicator.

4.3 Customer review

Legal framework

In some cases, customer due diligence needs to be repeated. Institutions are also required to keep their customer records up to date. These activities are referred to jointly as customer review.

Conducting customer due diligence

The *Wwft* prescribes in which cases an institution must conduct customer due diligence, as discussed in Chapter 3. Under certain circumstances, the *Wwft* requires institutions to repeat customer due diligence, namely:

- If there is an indication that the customer may be involved in money laundering or terrorist financing.
- If the institution doubts the truthfulness or completeness of data previously submitted by the customer.
- If this is justified by the risk that an existing customer may be involved in money laundering or terrorist financing.
- If there is an increased risk of money laundering or terrorist financing given the country where the customer resides or has its registered office.

Keeping customer records up to date

In addition, the *Wwft* requires the institution to take reasonable measures to keep the customer's records up to date. The customer file must be updated in any case if there is a relevant change to the customer's circumstances. The customer file should also be updated in any case if the *Wwft* requires the institution to contact the customer in order to assess the information relating to UBOs, and if the institution is required to do so under Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/79/EEC. In this respect, the institution should also include any signals that may give rise to a change in the customer's risk profile.[66] The EBA's ML/TF Risk Factors Guidelines provide further guidance on keeping customer records up to date.

When an institution applies simplified customer due diligence, the *Wwft* requires it to take reasonable measures to ensure that the data on the basis of which it has determined that simplified customer due diligence is sufficient, and the determination itself, are kept up to date. In the case of enhanced customer due diligence, the *Wwft* requires institutions to take reasonable measures to keep the data collected obtained as a result of taking enhanced customer due diligence measures up to date.

The following laws and regulations are particularly relevant:

- Section 3(5) of the *Wwft*
- Section 3(11) of the *Wwft*
- Section 6(3) of the *Wwft*
- Section 8(11) of the *Wwft*

The following other policy statement is particularly relevant:

- EBA ML/TF Risk Factors Guidelines

66 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 52.

Rationale
Customer reviews help institutions keep their risk profiles and underlying data up to date. This allows them to assess whether they are handling the risks posed by their customers appropriately, whether it is necessary to take additional mitigation measures or whether fewer mitigation measures will suffice.

Good practices

Good practice: review intensity policy
For each risk category, an institution has defined in its policy what data is relevant with regard to the identified risks and how often the data in the customer file should be updated. Depending on the risk and signals, the institution may suffice with consulting and analysing internal and external sources when conducting its review. Based on the circumstances, the institution assesses whether customer contact is necessary.

Good practice: periodic and event-driven review
The institution has defined its review frequency for each risk category. For higher-risk customers, the institution uses periodic reviews alongside event-driven reviews. For lower-risk customers, it only uses an event-driven review system. An event-driven review is a review that is conducted in response to a new development, such as a change in customer data, a signal about the customer from an external source or a transaction monitoring alert. The institution has adequate systems and processes in place to detect relevant developments.

The institution has stipulated that a review must in any case be conducted if:
- the customer wants to purchase a new service or product that involves new risks;
- the customer's transaction behaviour deviates from the expected transaction profile;
- there are signs that the customer has relocated to a high-risk jurisdiction;
- the customer becomes a PEP.

The institution has designed its operations (including its transaction monitoring system) to ensure that internal signals are detected in a timely manner, which in turn ensures that event-driven review triggers are detected in a timely manner. It regularly tests the effectiveness of this method, a process that is supervised by the compliance function.

Good practice: additional information and exit
During customer review, an institution finds that one of its customers must be designated as a PEP. In response, the institution takes the additional measures detailed in its policy and requests additional information. The customer refuses to provide the information. As this prevents the institution from completing enhanced customer due diligence with the desired result, it initiates its exit protocol. Pursuant to Section 16(4) of the *Wwft*, the institution also reports this to FIU-NL.

Good practice: changes in the organisational structure
An institution creates links with certain databases to be automatically informed of changes that are relevant to its customer review. For example, it has created a link between the Chamber of Commerce database and its customer registration system to stay informed of any changes in its customers' organisational structure. A report is generated when a director resigns or a new director is appointed, or when there is a shareholder change.

4.4 Termination of the business relationship

Legal framework

The *Wwft* provides that institutions must terminate a business relationship if they cannot meet the customer due diligence requirements (see the introduction to Chapter 3 and Section 4.3). As part of its customer due diligence, an institution must:

- Identify the customer and verify their identity (see Section 3.1.1);
- Establish whether the natural person representing the customer is authorised to do so and, where relevant, establish that natural person's identity and verify it (see Section 3.1.2);
- Take reasonable measures to verify whether the customer is acting on their own behalf or on behalf of a third party (see Section 3.1.3);[67]
- Identify the customer's UBOs and take risk-based and appropriate measures to verify their identity and, if the customer is a legal person, take risk-based and appropriate measures to gain an understanding of the ownership and control structure of the customer;
- Establish the purpose and the proposed nature of the business relationship (see Section 3.1.5);
- Continuously monitor its business relationships and the transactions conducted over the course of these relationships to ensure that these are in line with the institution's knowledge of its customers and their risk profiles (see Sections 4.1, 4.2 and 4.3), where necessary carrying out further investigations into the origin of the funds used in the relevant business relationship or transaction (see Section 3.1.6).

In addition, institutions are prohibited from continuing a correspondent banking relationship with a shell bank, or any other institution known to allow a shell bank to use its accounts.

Even if the *Wwft* does not expressly require an institution to terminate a business relationship, it may still choose to terminate the relationship if it has come to the conclusion that the relationship falls outside its risk tolerance.

For further guidance on the termination of business relationships, please refer to the EBA's ML/TF Risk Factors Guidelines and Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services.

FIU-NL reporting obligation for termination due to failure to meet customer due diligence requirements

If an institution terminates a business relationship because it cannot meet the customer due diligence requirements and there are indications that the customer in question is involved in money laundering or terrorist financing, the institution is required to report this to FIU-NL. In its report to FIU-NL, the institution must also provide a description of why the customer due diligence requirements have not been met and explain why there are indications of money laundering or terrorist financing.

The following laws and regulations are particularly relevant:

- Section 5(3), (4) and (5) of the *Wwft*
- Section 16(4), under b, and (5) of the *Wwft*

The following other policy statements are particularly relevant:

- EBA ML/TF Risk Factors Guidelines
- EBA Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services

67 Section 3(2) of the *Wwft*.

Good practices

Good practice: customer exit policy

An institution has drawn up a customer exit policy to ensure that relationships with existing customers are ended properly. In designing this customer exit policy, the institution followed the EBA's Guidelines on the policies and controls for the effective management of ML/TF risks when providing access to financial services. The policy states the circumstances under which the relationship with the customer will be terminated and the procedure for doing so (including timeframes). The institution monitors exit processes and takes action if the agreed timeframes are exceeded.

Good practice: termination due to suspicions of money laundering

A bank investigates a customer in connection with the purchase and sale of vehicles. This includes thorough open-source research on each counterparty, which reveals that parties that appear to be car dealerships have no online presence and are based in residential premises. A number of counterparties also stand out because they appear to be involved in a major fraud investigation. In addition, cars are procured by parties outside the car industry and the company receives rental and deposit payments for trucks, even though this is not listed as one of the company's business activities.

The institution is unable to get sufficient insight into the company's financial flows and notes that this prevents it from monitoring the business relationship on an ongoing basis. The institution initiates its exit protocol. Moreover, given the institution's suspicions that the company is involved in money laundering, it reports the company to FIU-NL in accordance with Section 16(4) of the *Wwft*.

Good practice: consequences of a Public Prosecution Service data requisition

Under the Code of Criminal Procedure, an institution may be ordered to disclose certain information about a customer or transaction. The institution has an obligation of confidentiality with regard to such requisitions, which are made by the prosecutor as part of a criminal investigation.

A requisition will usually prompt the institution to conduct enhanced customer due diligence and additional monitoring of the customer's transactions. The outcome of the enhanced customer due diligence may lead the institution to implement additional controls or to report unusual transactions to FIU-NL.

If the institution does implement controls, it ensures that these controls, and the communication about them, cannot be linked to information provided by the Public Prosecution Service, in accordance with the confidentiality obligation.

A requisition from the Public Prosecution Service does not have to be a reason for the institution to terminate the customer relationship under the *Wwft* or Wft, or to suspend its services. If there are unacceptable risks, or if the customer due diligence requirements cannot be met, the institution must terminate the customer relationship.

However, the prosecutor may request the institution to continue the customer relationship and transactions for the benefit of the criminal investigation. In this situation, enhanced monitoring of the customer and their transactions, and careful documentation of the relevant facts and circumstances in the customer file, provide safeguards to mitigate potential risks.

5 Recording data, retention obligations and protection of personal data

This chapter covers data capture and retention and the protection of personal data. The *Wwft* obligations regarding the recording of data, retention obligations and the protection of personal data apply to both initial customer due diligence (Chapter 3) and ongoing monitoring (Chapter 4).

Legal framework

The *Wwft* requires institutions to keep the documents and data used for customer due diligence on file in a retrievable manner. It also specifies which documents and data must always be retained. Institutions must store these documents and data in an accessible manner for a period of five years from the time of termination of the business relationship or from the execution of the transaction. These obligations cover both the documents and data an institution has used for its own customer due diligence and, in the case of introductory customer due diligence, the documents and data it has obtained from the introducing institution. Information obtained in the context of simplified or enhanced customer due diligence must also be retained by institutions.[68] Moreover, institutions must have systems in place that enable them to respond promptly and adequately to inquiries from FIU-NL and the supervisory authority. These systems should provide secure channels to ensure the confidentiality of requests from FIU-NL and the supervisory authority.

In addition, the *Wwft* stipulates that institutions must record data relating to an unusual transaction report in a retrievable manner. The retention period is five years from the time the report is submitted to, or received by, FIU-NL.

68 *Parliamentary Papers II*, 2017-2018, 34 808, no. 3, p. 79.

Furthermore, the *Wwft* provides that institutions may only process personal data collected under the *Wwft* for the purpose of preventing money laundering or terrorist financing. This personal data may not be processed for commercial purposes, or for other incompatible purposes. Before an institution enters into a business relationship or carries out a non-recurring transaction, it must inform the customer of its legal obligations under the *Wwft* with regard to the processing of personal data, such as the retention period. Upon expiry of the retention period, the institution must immediately destroy all personal data obtained under the *Wwft*, unless otherwise provided by law. In doing so, the institution is bound by the provisions of the GDPR.

The following laws and regulations are particularly relevant:
- Section 33 of the *Wwft*
- Section 34 of the *Wwft*
- Section 34a of the *Wwft*
- GDPR

The following policy statements are particularly relevant:
- EBA ML/TF Risk Factors Guidelines

Rationale
By recording and retaining documents and data, institutions are able to gain insight into what risks a customer does or does not pose, and to provide this insight to the supervisory authority. This may affect how much attention an institution chooses to pay to a customer. As such, the recording and retention of data serves partly to demonstrate internally and to the competent authority that an institution has taken appropriate action given the risks it has identified.

Customer due diligence data is also documented to facilitate reporting to FIU-NL or for complying with orders from an investigative authority.

Good practices

Good practice: recording documents and data in customer file
An institution records all documents and data related to customer due diligence in its customer files. For example, if a reference group is used in establishing the purpose and intended nature of the relationship, this is recorded in the customer file. These customer files are easily accessible to staff, including to analysts within the institution who assess signals from transaction monitoring, and to the compliance function.

Good practice: weighing up interests
In addition to the obligations of the *Wwft*, an institution's policy on the collection and retention of data and documents takes sufficient account of other interests, in particular the importance of privacy. To safeguard these interests, the institution decides to involve the data protection officer in shaping the policy on data collection and retention.

6 Miscellaneous

This chapter discusses a number of topics that could not be properly accommodated in one of the other chapters because they relate to obligations that do not follow directly from the Wwft but are closely related to it, namely with regard to protected accounts (Section 6.1) and the reporting of wrongdoing (Section 6.2).

6.1 Protected accounts

Legal framework
The Regulation on Protected Accounts under the *Wft* (*Regeling afgeschermde rekeningen Wft*) sets out a procedure for banks and branches with regard to existing and yet to be opened protected accounts.

A protected account is an account that may hold a balance in cash, securities, precious metals or other securities, where the customer's identity is not visible in the processing of transactions or is otherwise protected by the use of only an account number, number or code word. The customer's identity (which may be temporary or assumed) is known to the bank or branch. The words "temporary or assumed" mean that the persons referred to in Section 44(1) of the Police Act 2012 and Section 15(2) of the Intelligence and Security Services Act 2017 also fall within the scope of the Regulation.[69]

Accounts may be protected from the bank or branch's own staff in order to protect the privacy and security of the customers concerned, or to prevent the use of inside information. This therefore serves legitimate interests.[70]

The bank or branch must have a restrictive policy on the opening of protected accounts and provide adequate instructions to staff on the opening and management of protected accounts.

The Regulation requires the bank or branch – without prejudice to its obligations under the *Wwft* – to maintain a central register when using protected accounts. This register must contain at least the data relating to customer due diligence that must be recorded under the *Wwft* (see Section 5.1), and it must provide access at least by name and number or code key. The compliance function must also have access, and the bank or branch must appoint an administrator.

The Regulation only covers identity protection during transaction processing. The *Wwft*'s customer due diligence requirements apply without prejudice, as do the requirements of the WTR2.

The following laws and regulations are particularly relevant:
- Section 14(6) of the Decree on Prudential Rules for Financial Undertakings
- Regulation on Protected Accounts under the *Wft*

Rationale
In a limited number of cases, it may be desirable to offer a customer a protected account, for example for security or privacy reasons, or to serve the public interest. This is why we created the Regulation on Protected Accounts under the *Wft*. Institutions should have restrictive policies on opening these accounts.

6.2 Reporting wrongdoing

Legal framework
The *Wwft* stipulates that institutions must have adequate procedures, appropriate to their nature and size, that allow their employees to report a breach of the *Wwft* internally and anonymously through a specific, independent channel.

People who report wrongdoing are protected under the Whistleblower Protection Act (*Wet bescherming klokkenluiders*). Like the *Wwft*, the Whistleblower Protection Act requires institutions to have an internal procedure for reporting suspected wrongdoing within the organisation. The Whistleblower Protection Act sets out a number of rules for the design of this procedure. Institutions, regardless of their size, must always comply with the requirements of the Whistleblower Protection Act regarding the internal reporting procedure.

69 *Government Gazette* 2018, 57233. For more information on the protection of the identity of these persons, see *Parliamentary Papers II*, 2010-2011, 30 880, 11, p. 77 in conjunction with *Parliamentary Papers II*, 1998-1999, 26 461, 7, p. *Parliamentary Papers II*, 2016-2017, 34 588, no. 3, p. 26
70 *Government Gazette* 2006, 244, p. 31.

The Whistleblower Protection Act designates DNB as the authority responsible for receiving and investigating reports of suspected wrongdoing at financial institutions. Wrongdoing or suspected wrongdoing can be reported to our Integrity Reporting Desk.[71] Examples of wrongdoing include fraud, corruption, conflicts of interest, money laundering or the provision of services without a licence from DNB.

The following laws and regulations are particularly relevant:

- Section 20a of the *Wwft*
- Section 2 of the Whistleblower Protection Act
- Sections 2c and 2d of the Whistleblower Protection Act

Rationale

It is important that cases of wrongdoing and suspected wrongdoing in the financial sector are reported and investigated, as this contributes to both an ethical sector and financial stability.

71 More information on reporting wrongdoing can be found on the DNB website.

Abbreviations

AI/ML model	Artificial intelligence/machine learning model
(A)ML	(Anti-)Money Laundering
(C)FT	(Countering) Financing of Terrorism
AMLD	Anti-Money Laundering Directive
AP	Dutch Data Protection Authority
GDPR	General Data Protection Regulation
Bpr	Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft*)
EBA	European Banking Authority
eIDAS	Electronic Identification, Authentication and Trust Services Regulation
FATF	Financial Action Task Force
FIU-NL	Financial Intelligence Unit
HRTC	High-Risk Third Country
MiCAR	Markets in Crypto Assets Regulation
NRA	National Risk Assessment
PPS	Public Prosecution Service
PEP	Politically exposed person
SIRA	Systematic integrity risk analysis
SNRA	Supranational Risk Assessment
Sw	Sanctions Act (*Sanctiewet 1997*)
TFR	Transfer of Funds Regulation
UBO	Ultimate Beneficial Owner
Wft	Financial Supervision Act (*Wet op het financieel toezicht*)
WTR2	Wire Transfer Regulation (2)
Wtt 2018	Act on the Supervision of Trust Offices 2018 (Wet toezicht trustkantoren 2018)
Wwft	Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*)

Glossary

Term	Explanation
Alert	An alert is a signal indicating a potentially unusual transaction. This includes transactions that fall outside the expected pattern and/or profile, as well as transactions that have no economic or legal purpose.
Alert handling	Institutions must investigate alerts (and combinations of alerts) to assess whether the transaction in question is in fact unusual.
Policy	Guidelines, procedures and measures referred to in Section 2c of the *Wwft*.
Desk research	The collection and analysis of pre-existing data in order to answer the research question.
Business rule	A business rule is a detection rule based on scenarios and threshold values with regard to relevant money laundering and terrorist financing risks. An institution can use business rules in its transaction monitoring system. Business rules are used to generate alerts for unusual transactions.
Threshold value	A specified minimum or maximum value.
Typology	Characteristics, or groups of characteristics, that point to money laundering or terrorist financing.
Risk tolerance	An institution's risk tolerance indicates which integrity risks it considers acceptable after controls have been implemented and which risks it does not want to be exposed to.
Pre-transaction monitoring	Transaction monitoring before a transaction is completed.
Post-transaction monitoring	Transaction monitoring after a transaction has been completed.
Wwft policymaker	The institution's day-to-day policymaker who bears responsibility for compliance with the *Wwft*.
Name-number check	Checking the combination of the customer's name and account number.
Three lines of defence	An organisational structure consisting of a first line, second line and third line, where each line has its own tasks and responsibilities with regard to assessing and managing risks within the institution.

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 (0) 20 524 91 11
dnb.nl/en

Follow us on:
LinkedIn
Twitter
Instagram

DeNederlandscheBank

EUROSYSTEEM