DNB Wwft Q&As and Good Practices

(consultation version)

DeNederlandscheBank

EUROSYSTEEM

Inhoud

1 Introduction

In addition to solidity, integrity is a prerequisite for a sound financial system. De Nederlandsche Bank (DNB) conducts integrity supervision of a wide range of financial and other institutions. The purpose of integrity supervision is, among other things, to prevent the use of the financial system for money laundering and terrorist financing purposes. The framework for this is primarily laid down in the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*). With this Q&As/Good Practices document, DNB aims to offer financial institutions more information about their legal obligations under the *Wwft*. The *Wwft* implements the European directive aimed at preventing money laundering and terrorist financing (AMLD).[1] This Directive is partly based on the recommendations of the Financial Action Task Force (FATF). Besides the *Wwft*, the integrity supervision conducted by DNB is based on the Pensions Act (*Pensioenwet – Pw*), the Act on the Supervision of Trust Offices 2018 (*Wet toezicht trustkantoren 2018 – Wtt*) and the Sanctions Act 1977 (*Sanctiewet – Sw*).[2]

With these 'Q&As and Good Practices Wwft', DNB aims to provide guidance on the legal obligations regarding the prevention of money laundering and terrorist financing. This document replaces the previously published DNB Guidance on the *Wwft & Sw*, with the exception of the sections on the Sanctions Act. The present document focuses only on anti-money laundering and terrorist financing regulations, which are primarily laid down in the *Wwft*.[3]

Supervision of compliance with the *Wwft* has been assigned to DNB for the following types of entities: banks, life insurers, payment service providers and agents, electronic money institutions, crypto service providers,[4] exchange institutions, trust offices[5] and other financial institutions[6] and certain branch offices.[7] Trust offices must meet additional requirements, which are not specified in the present document.[8]

Status of Q&As

Q&As published by DNB provide further insight into implementation and application of statutory supervisory rules. Entities subject to our supervision may choose to comply with the laws and regulations in other ways, however. If they do so, they must be able to demonstrate and substantiate their compliance. To read more about the status of our policy statements, go to the Explanatory guide to DNB's policy statements on Open Book on Supervision.

1 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 purposes 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 Directive 2006/70/EC of the Commission, OJEU 2015, L 141/73, as subsequently amended.
2 Additionally, DNB conducts integrity supervision over institutions in the Caribbean Netherlands, subject to its specific laws and regulations.
3 The section concerning the Sanction Act (Sw) that is currently included in the DNB Guideline for the Wwft & Sw (DNB Leidraad Wwft & Sw) will be re-published in a separate document, pending the new legal framework.
4 As included in Section 1a(4), under l and m, of the *Wwft*.
5 Trust offices in particular are also subject to the *Wtt 2018*. This means that additional requirements apply to trust offices which are not covered in this document.
6 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.
7 These are branches in the Netherlands of banks, payment service providers, electronic money institutions, exchange institutions, life insurers and other financial institutions included in Section 1a(3), under a, of the *Wwft*.
8 The Good Practices for the trust sector are currently under review.

Status of Good Practices

Good practices set out suggestions or recommendations for entities. They are examples of possible applications that, in DNB's opinion, provide a good interpretation of the obligations laid down in legislation and regulations. Good practices are indicative and entities are free to take a different approach, as long as they otherwise comply with the laws and regulations and are able to demonstrate and substantiate their compliance. To read more about the status of our policy statements, go to the Explanatory guide to DNB's policy statements on Open Book on Supervision.

From recovery to balance

By publishing this Q&As/Good Practices, DNB is following the recommendations in the report on the banking sector 'From recovery to balance'.[9]

In this report, DNB argued that financial and economic crime could be combated more effectively if financial institutions and supervisory authorities were to adopt a more risk-based approach. In addition, it called for a smarter application of data-driven technological innovations and stressed the need for more focused cooperation throughout the chain. These efforts must not be dominated by the fear of making mistakes. Rather, they must engender confidence that working closely together with all parties involved is the best way to prevent and combat financial crime in the Netherlands.[10]

Boosting effectiveness primarily means that less criminal money will find its way into the financial infrastructure, as criminals will be stopped at the gate more frequently. And when criminal money does enter the system, improved detection measures will result in more convictions and confiscations. Boosting efficiency in the fight against financial crime means reducing the administrative burden on banks as well as their customers where possible. An effective and efficient strategy can be achieved through a more risk-based approach by both entities and supervisors.

This Q&As/Good Practices document underlines the goal of the *Wwft*: to ensure effective gatekeeping to prevent the financial system from being used for money laundering and terrorist financing. The measures taken by entities under the *Wwft* should contribute to that goal – and thus are in principle not an end in themselves. The Wwft also imposes obligations on entities where there is no room for a risk-based approach. Naturally, entities must adhere to these obligations.

9 DNB (2022), *From recovery to balance: A look ahead to a more risk-based approach to preventing and combating money laundering and terrorist financing*, 2022. (www.dnb.nl/media/2ambmvxt/van-herstel-naar-balans.pdf).
10 DNB (2022), *From recovery to balance: A look ahead to a more risk-based approach to preventing and combating money laundering and terrorist financing*, 2022, p. 3.

Overview

This document is structured as follows:

Chapter	Title	Explanatory notes
1	Introduction	
2	Context	This chapter discusses the framework within which entities must establish compliance with the *Wwft*. The risk management cycle, or compliance cycle, is central to this. Other topics discussed include outsourcing, obligations under the Wire Transfer Regulation 2 (WTR2), malpractice reporting and personal data protection.
3	Customer due diligence: customer acceptance	This chapter discusses the customer acceptance process entities must complete under the *Wwft*. It covers the various components of customer due diligence, such as identifying and verifying the customer and UBO, and investigating the source of funds. Higher- and lower-risk situations are also discussed.
4	Customer due diligence: ongoing monitoring	This chapter focuses on two parts of ongoing monitoring, namely transaction monitoring and customer review.
Annex I	Abbreviations	This annex provides a list of commonly used abbreviations.

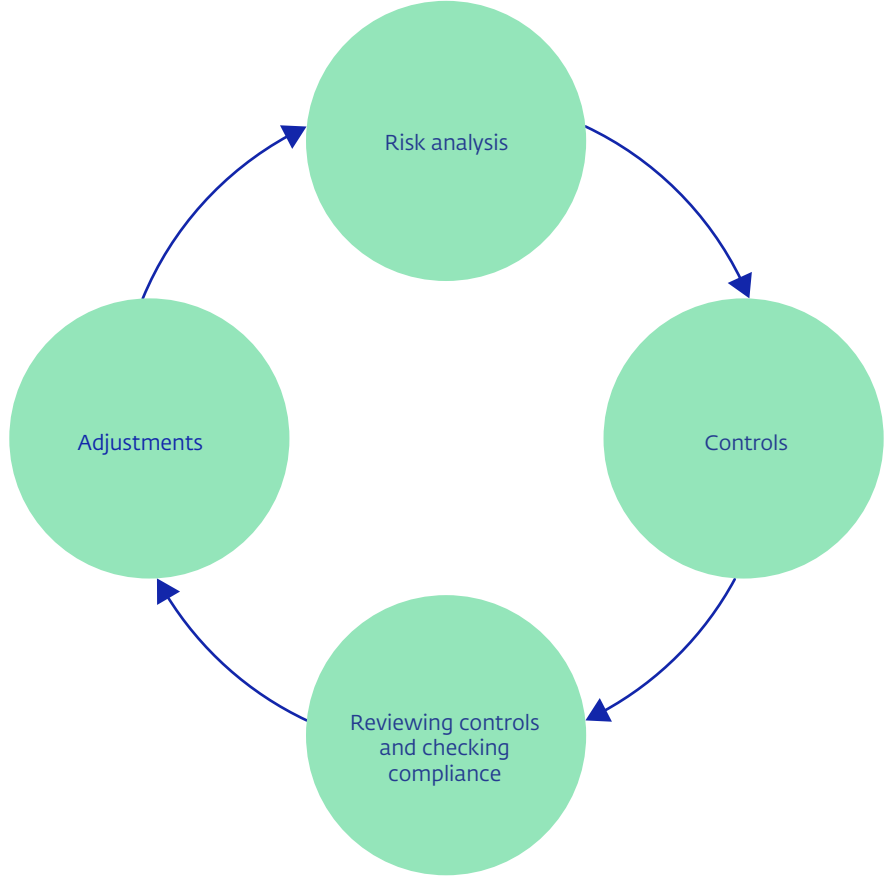
2 Context

2.1 Risk management and operations

The purpose of the *Wwft*, as its name implies, is to prevent money laundering and terrorist financing. The act, which stipulates a risk-based approach,[11] aims to ensure that entities take appropriate measures to adequately manage their risks of involvement in money laundering and terrorist financing.

Where possible, the intensity of measures to prevent money laundering and terrorist financing should be tailored to specific risks. For instance, high-risk customers will require more attention, while less intensive monitoring suffices for lower-risk customers.

The risk-based approach should start with a risk analysis. Based on the outcome of this analysis, the entity in question can identify appropriate management measures. It is also important that the entity reviews its compliance with these measures, as well as their effectiveness, making adjustments where necessary. Below is a schematic representation of a risk-based approach as prescribed by the *Wwft*:



In performing its supervisory task, DNB assesses entities' compliance with the *Wwft*. This involves a comprehensive review of the risk-management system.

11 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 8.

2.1.1 Risk analysis

Sound risk analysis is crucial in preventing financial crime. The risk analysis identifies the main integrity risks entities are exposed to as a result of their operations. If an entity has a good understanding of the integrity risks it runs, both within its own organisation and with regard to its customers, it can base its approach on these insights.[12] Moreover, without a proper risk analysis it is impossible to determine whether an institution's control measures are appropriate for the relevant operations.

The analysis that identifies and assesses money laundering and terrorist financing risks can be used as a steering document by management.

- The risk analysis provides insight into the most significant perceived integrity risks for the entity in question (top risks).
- Based on this analysis, the entity then determines its key priorities and what actions it should initiate accordingly to mitigate its top risks.

This also means that the risk analysis should be the starting point for establishing policies, consisting of procedures and measures, to effectively mitigate and control the identified risks. Compliance with these policies is monitored by the compliance function. Additionally, the intensity of the execution of the audit function is aligned with the risk analysis.[13]

Q&A

QA.2.1: Question

How does the *Wwft* risk analysis fit into the SIRA?

Answer

SIRA stands for systematic integrity risk analysis. The Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*) stipulates that entities must ensure a systematic analysis of integrity risks.[14]

QA.2.2: Question

The *Wwft* risk analysis is limited to entities' exposure to the risk of money laundering and terrorist financing, while the SIRA has a broader scope. It makes sense to include the *Wwft* risk analysis in the SIRA, but this is not mandatory, when an entity has the legal obligation to establish a SIRA.[15]
What does a risk analysis involve?

Answer

The types of risk to which an entity is exposed depend on the nature of its operations. This means that a risk analysis is first and foremost specific to the institution, focusing on the risks associated with its activities.

Any risks related to money laundering or terrorist financing can be further identified by, for instance, conducting a proper analysis of the risks in the client portfolio, as well as by assessing how each risk might affect the entity and what the negative consequences of ineffective risk management could be.

12 Section 2b of the *Wwft*; Section 2c(1) and (2) of the *Wwft*.
13 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 8, 43-45
14 Section 10(1) of the *Bpr*.
15 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 43.

Examples of negative consequences include the 'contamination' of the financial system with criminal funds and the transfer of funds for the purpose of financing terrorist activities.

After the risk analysis has been completed, it is possible to determine which control measures can sufficiently mitigate the identified risks.

For further guidance and tools, see DNB's SIRA Good Practices.[16] The SIRA methodology can also be used to develop money laundering and terrorist financing risk assessment processes.

QA.2.3: Question

What risk factors should a risk analysis take into account?

Answer

The risk factors – indicators pointing to the presence of specific risks – depend on the institution's profile and the services it provides. When identifying and assessing *Wwft* risks, an entity 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.[17]

Money laundering and terrorist financing risks occur at different levels:

- At European Union level, the supranational risk assessment is available.[18]
- At national level, the national risk assessment is available.[19]
- Each entity has its own institution-level risk assessment.[20] In doing so, the entity has to, at a minimum, take into account the risks associated with types of clients, products, services, transactions, delivery channels and with countries or geographic areas.[21]

Within an individual client investigation, an institution also takes into account the risks that arise in that specific case. The entity aligns their client investigations with the risk sensitivity associated with the type of customers, business associates, products and transactions.[22]

The risk assessment referred to here is the entity-level risk analysis. The following should be noted here:

- Although the supranational and national risk assessments have a different scope than the institution's individual risk analysis, the entity should also consider these to establish effective policies, procedures and measures.[23]
- The risks associated with customers, business associates, products and transactions influence the institution's risk profile. These risks can be identified, assessed and substantiated through portfolio analysis.

16 Link: https://www.dnb.nl/media/pfmbzrah/guidance-integrity-risk-analysis-english-version.pdf. This document is scheduled for review in the near future.
17 Section 2b(2) of the *Wwft*.
18 Link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554
19 Money Laundering NRA, Terrorist Financing NRA.
20 Section 2b(1) of the *Wwft*.
21 Section 2b(2) of the *Wwft*.
22 Section 3(8), (9) of the *Wwft*.
23 Section 2c(1) of the *Wwft*. *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 43.

QA.2.4: Question
How often should a risk analysis be updated?

Answer
There is no specific time frame for this. Entities are expected to keep their risk identification and assessment methods up to date by conducting risk analyses at regular intervals and in response to significant changes, for example to the services provided or business operations. The risk analysis should enable the entity to adequately manage the risks identified.[24]

In other words, the process is cyclical. The interval between risk analysis reviews should be informed by the nature of the institution's operations (factors such as customer turnover, transactions and the introduction of new products) and relevant external developments (such as geopolitical developments or changes in legislation).

QA.2.5: Question
Incidents or media attention may also warrant a risk analysis update.
Who is responsible for the risk analysis?

Answer
The risk analysis looks at the risks the entity faces and underpins effective risk management. The entity is responsible for compliance with the *Wwft*.
The risk analysis is an important control instrument for the board, upon which the further design of the entities' control measures (see 2.1.2) is based. This makes the risk analysis important for the other job functions within the entity as well.

QA.2.6: Question
How extensively should risks be analysed?

Answer
The risk analysis should provide an assessment of the integrity risks a specific entity faces in its operations. This means that any risks related to money laundering and terrorist financing should be identified and mapped.

The risk assessment should be tailored to the nature and size of the institution.[25] The risk analysis must enable the entity to take appropriate control measures;[26] more where necessary, less where possible.

GP2.1: Good practice - risk analysis maintenance
An entity has set up a process to ensure that lessons learned from incidents, but also FIU reports and thematic analyses, for example, are included in the periodic update of the risk analysis. The risk analysis is immediately recalibrated in response to major incidents. Depending on the role, each job function within the entity contributes to a sound risk analysis. This is documented during the process of development and updating of the risk analysis.

GP2.2: Good practice - customer portfolio analysis
An entity conducts an in-depth analysis of its customer portfolio to determine its exposure to customer groups or sectors that inherently pose a higher risk with regard to money laundering and/or terrorist financing. The results of this analysis are used in the risk analysis.

For more examples, please refer to the SIRA Good Practices.[27]

24 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 43.
25 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 42
26 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 43.
27 Link: https://www.dnb.nl/media/pfmbzrah/guidance-integrity-risk-analysis-english-version.pdf. This document is scheduled for review in the near future.

2.1.2 Controls

The risk analysis identifies the main money laundering and terrorist financing risks entities are exposed to as a result of their operations. To effectively manage and mitigate these risks, an entity should have policies, procedures and measures in place.[28] These are jointly referred to in this Q&As/ Good Practices as "controls".

These (controls) are approved by the day-to-day policymakers.[29]

Q&A

QA.2.7: Question
Does the *Wwft* prescribe the same controls for every institution?

Answer
No. The control measures adopted by the entity must be proportionate to the nature and size of the entity.[30] The control measures should therefore be appropriate to the size and nature of the entity, and aimed at effectively managing and mitigating money laundering and terrorist financing risks. This means that high-risk entities will usually have more extensive control measures than low-risk entities. Controls are thus institution-specific.

Control measures taken by the entity must be based on a risk analysis.

QA.2.8: Question
Are there elements that should always be covered by control measures?

Answer
The *Wwft* stipulates that entities must have policies, procedures and measures in place to effectively manage and mitigate the risks of money laundering and terrorist financing.[31] They must address, in addition to the money laundering and terrorist financing risks to which an entity itself is exposed, risks that are relevant to the entity that are identified in supranational risk assessment and national risk assessment.[32]

The control measures should at least cover the entities' obligations regarding:
- risk management (Section 1f t/m 2d of the *Wwft*)
- groups (Section 2e and 2f of the *Wwft*)
- customer due diligence (Sections 3-11 of the *Wwft*)
- reporting unusual transactions (Sections 16-20 of the *Wwft*)
- retention of documentary evidence (Sections 33-34a of the *Wwft*)
- vetting and training of employees (Section 35 of the *Wwft*).[33]

28 Section 2c(1) of the *Wwft*.
29 Section 2c(3) of the *Wwft*.
30 Section 2c(2) of the *Wwft*.
31 Section 2c(1) of the *Wwft*.
32 Section 2c(1) of the *Wwft*; *Parliamentary Papers II* 2017-2018, 34 808, nr. 3, p. 43.
33 Section 2c(2) of the *Wwft*.

QA.2.9: Question
Why do employees need training?

Answer
Entities must ensure that employees are familiar with the provisions of the *Wwft* to the extent that this is relevant to the performance of their duties, and taking into account the institution's risks, nature and size.[34] Employees should also be able to recognise and handle unusual transactions.[35]
Training and education are important in a risk-based approach, as this (the risk based approach) is largely dependent on the institution's (policymakers and employees) judgment.[36]
This means that adequate knowledge, awareness and experience on the part of employees concerning the management of the risks of money laundering and terrorist financing are important prerequisites for an effective control framework.

QA.2.10: Question
Should employees be screened?

Answer
Entities must ensure that employees are screened as relevant to the performance of their duties and taking into account the institution's risks, nature and size.[37]
In its recommendations, the FATF indicates that entities should have adequate "screening procedures" to ensure high standards when hiring new staff. These procedures should be appropriate to the institution's risks, nature and size, as well as to the employees' duties.[38]

The screening authority Justis offers employee screening guidelines on its website.[39]

GP2.3: Good practice - education & training

Because integrity risks are dynamic and controls are adjusted accordingly, entities must regularly evaluate and update their training courses. To enable staff to keep abreast of new developments and to improve awareness in the long term, entities must provide training courses at regular intervals.

The training courses must be tailored to the institution's various functions.
- CDD analysts must learn how to conduct customer due diligence properly and completely, and how to identify red flags in time.
- Compliance staff must attend additional training courses to stay up to date on developments with regard to money laundering and terrorist financing risks, and on relevant laws and regulations.
- Day-to-day policymakers must receive training to help them fulfil their responsibilities.
- Staff tasked with recruiting customers and selling products must receive training on the provisions of the *Wwft*, ensuring that they take these into account when carrying out their work.

Besides offering mandatory e-learning modules and on-site training, the entity should organise regular knowledge sessions where money laundering techniques, methods and trends are discussed, and where employees can discuss specific cases.

The entity keeps records of 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.

34 Section 35 of the *Wwft*.
35 *Parliamentary Papers II*, 2007–2008, 31 238, no. 3, p. 35.
36 *Parliamentary Papers II*, 2007–2008, 31 238, no. 3, p. 35.
37 Section 35 of the *Wwft*.
38 FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, 2012-2023, p. 85.
39 www.justis.nl/producten/verklaring-omtrent-het-gedrag-vog/documenten-vog.

2.1.3 Reviewing controls and checking compliance

It is important that entities actually use the controls in place.[40] In addition, the controls must effectively manage and mitigate risks.

In this context, the *Wwft* prescribes that an entity ensures systematic review of policies, procedures and measures.[41] When present, the compliance function verifies compliance with internal rules established by the entity and legal requirements.[42] When present, an audit function evaluates the performance of the compliance function in addition to monitoring compliance with rules stipulated in the *Wwft*. [43]

Q&A

Q.A.2.11: Question
What is systematic review?

Answer
The entity must regularly ("systematically") test its controls and make adjustments where necessary. Updates to the risk assessment should also inform these changes.[44]
During a review, the entity thus checks whether the controls effectively manage and mitigate risks. In doing so, the entity also considers whether the risks it is exposed to have changed, and whether the controls need to be adjusted accordingly. This is documented by the entity.

Q.A.2.12: Question
What kind of audits and reviews should the compliance function perform?

Answer
If an entity has an independent compliance function, this should monitor compliance with statutory rules and internal regulations drawn up by the entity itself.[45] This involves, among other things, ensuring that procedures, such as customer due diligence, are carried out in line with applicable regulations.[46]

In addition, the compliance function also plays a role in the review process, checking whether the controls in place are effective.

Q.A.2.13: Question
Is every entity required to have an independent compliance function?

Answer
This depends on the institution's size and nature.[47]
For smaller entities, maintaining an independent compliance function may be disproportionately burdensome and therefore inappropriate. The size and type of entity also play an important role in compliance with this requirement.[48]

40 Sections 2c(4), 2d(3) and (4) of the *Wwft*. Cf. ECLI:NL:RBROT:2015:BQ4969
41 Section 2c(4) of the *Wwft*.
42 Section 2c(3) of the *Wwft*.
43 Section 2d(4) of the *Wwft*.
44 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 44.
45 Section 2d(3) of the *Wwft*.
46 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 44.
47 Section 2d(2) of the *Wwft*.
48 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 44.

The way in which the compliance function is set up can also be aligned with the nature and the size of the institution. The compliance function should be performed in an independent and effective manner. In principle, this means that people who are involved with performing the compliance function are not also involved with the activities they supervise. However, in the case of smaller entities, it can be disproportionately burdensome to ensure the independence of the compliance function in this way. Ultimately, the institution's board is responsible for monitoring compliance with the *Wwft*.

Depending on their nature and size, entities may also choose to outsource the compliance function (in whole or in part).[49]

Q.A.2.14: Question
What is the role of the audit function in relation to the *Wwft*?

Answer
Where applicable and insofar as is appropriate to its nature and size, the entity must ensure the independent performance of an audit function with respect to its activities.[50]
The audit function independently assesses the institution's compliance with the *Wwft* and the performance of the compliance function. This at least includes an assessment of the control measures. The intensity of the audit function's activities should be aligned with the institution's risk profile. The extent to which the audit function is independent depends on the nature and size of the institution.[51]
Like the compliance function, the audit function can also be outsourced (in whole or in part).[52]

GP2.4: Good practice - compliance function

An entity has defined the position of its compliance function in a compliance charter. This stipulates, among other things, that the compliance officer has access to all 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 drafting the charter, the entity used the EBA guidelines on this subject.[53]

GP2.5: Good practice - audit function

An entity 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 entity must use these findings to tighten its controls where necessary. The audit function should then determine whether these interventions are sufficient.

GP2.6: Good practice - review of training courses

An entity has a *Wwft* training programme for its employees. Every year, the compliance function tests the effectiveness of this training programme by checking whether employees know the risks relevant to their jobs, whether they recognise concrete examples of these risks and whether they take appropriate action. The compliance function performs this test on the basis of actual customer files and transaction records, among other things.

49 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 44. Under Section 16(2) of the *Wtt 2018*, trust offices are not allowed to outsource the compliance function.
50 Section 2d(4) of the *Wwft*.
51 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 45.
52 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 44.
53 www.eba.europa.eu/eba-publishes-guidelines-role-and-responsibilities-amlcft-compliance-officer.

2.1.4 Adjustments

The systematic review and compliance monitoring may show that the controls are appropriate, and that they effectively manage and mitigate money laundering and terrorist financing risks.

Alternatively, they may find that:

- the controls do not sufficiently manage and mitigate money laundering and terrorist financing risks;
- compliance with the controls is insufficient.

If shortcomings are found, the entity must ensure compliance by adjusting the controls to align them with the relevant risks.[54]

GP2.7: Good practice - making adjustments

An institution's compliance function has identified inadequate compliance with policies, procedures and measures within a department, exposing the entity 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 board member responsible for compliance with the *Wwft* and the audit function also receive this report.

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*-responsible director.

2.2 Outsourcing

Under certain conditions, entities can outsource parts of the customer due diligence process. However, the outsourcing entity always remains fully responsible for complying with customer due diligence requirements. This means that the outsourcing entity must establish effective controls to ensure that customer due diligence is carried out. Final decisions on whether to accept customers and costumers' risk levels are always (verifiably) made by the institution.

Q&A

QA.2.15: Question

Which parts of the customer due diligence process are entities allowed to outsource?

Answer

Pursuant to Section 10 of the *Wwft*, entities are allowed to outsource parts of the customer due diligence process under an outsourcing or agency agreement.

Entities may outsource the following parts of the customer due diligence process outlined in Section 3(2) of the *Wwft*:

a. customer identification and verification;
b. UBO identification and verification;
c. identification of purpose and intended nature of the business relationship;
d. verification of competence and identity of the customer's representative;
e. investigation of whether a customer is acting on their own behalf, or on behalf of a third party.

54 Section 2c(4) of the *Wwft*. *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 44-45.

It is important to note here that the outsourcing entity remains responsible; the party to which the services are outsourced always acts on behalf of the outsourcing institution. This means that the outsourcing entity bears responsibility for any errors and omissions in the customer due diligence, and for the associated risks. The entity also remains responsible for keeping customer data up to date.

QA.2.16: Question
What is the difference between outsourcing and introducing?

Answer
If an entity wants to introduce a customer for which it has already conducted due diligence to another institution, Section 5(1) of the *Wwft* stipulates under which conditions the accepting entity may rely on the customer due diligence of the introducing institution. This is different from outsourcing customer due diligence under Section 10 of the *Wwft*. In this situation, the entity outsources (part of) the business process to a third party that executes this (part of the) process on the entity's behalf. When introducing a client based on Section 5 of the *Wwft*, an entity may make use of the investigation conducted by another entity that has an independent obligation under the *Wwft* to carry out client due diligence.

QA.2.17: Question
For which parts of the customer due diligence process is outsourcing not allowed?

Answer
The entity may not outsource the ongoing monitoring of business relationships and transactions. These must be monitored by the entity itself.

QA.2.18: Question
What requirements should outsourced customer due diligence meet?

Answer
If the entity proceeds to outsource customer due diligence, it must conduct a risk assessment and document its findings. This includes an assessment of the expertise of the third party and how this third party complies with the *Wwft* on behalf of the institution.
Furthermore, it is important that the entity not only establishes that the third party performing the customer due diligence (in whole or in part) complies with the *Wwft* and, where necessary, with the institution's internal policies, but also that the entity periodically checks and confirms this.

QA.2.19: Question
Are Dutch licensed entities subject to any other outsourcing requirements?

Answer
Yes, they are. Dutch entities licensed by DNB under the *Wft* are subject to additional requirements that are also relevant when outsourcing parts of the customer due diligence process. For example, Section 3(17) of the *Wft* stipulates that the organisation must be structured in such a way as to ensure sound and ethical business operations. Section 3(18) of the *Wft* provides rules for outsourcing. The requirements set for outsourcing based on these rules are detailed in Chapter 5 of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels - Bpr*).

GP2.8: Good practice - outsourcing policy

An entity has properly identified the implications of potential outsourcing and has drawn up a comprehensive general outsourcing policy. The entity regularly reassesses its outsourcing policy, considering whether outsourcing puts it at risk of inadequate compliance with the *Wwft*.

Before selecting a service provider, the entity conducts an evaluation to ensure that the service provider will carefully execute the work to be outsourced. The entity documents this in writing in a due diligence assessment.

The decision to outsource *Wwft* activities is taken by management. The day-to-day policymaker overseeing compliance with the *Wwft* is also involved in decisions on outsourcing parts of the customer due diligence process to the service provider.

The entity chooses to outsource certain parts of the customer due diligence process to a service provider outside the European Economic Area. Given the risks that this may involve, the entity pays particular attention to a number of key issues. These include the protection of confidential (personal) data and ensuring that it can effectively supervise the service provider to which the processes have been outsourced.

GP2.9: Good practice - outsourcing agreement

For each component, the outsourcing agreement describes the duration of the outsourced activities and how the activities are to be performed. The outsourcing agreement must include a clause that explicitly stipulates that supervisory authorities have the right to access and investigate relevant third-party data and premises if necessary.

Moreover, the entity must ensure that its outsourcing policy and the outsourcing agreement state whether the third party may outsource activities itself. If the outsourcing agreement allows further subcontracting, it must include requirements for this. These must at least include the same requirements that the third party must comply with itself, such as the outsourcing party's right of instruction and the right to direct access and investigation.

GP2.10: Good practice - assessment of outsourcing implementation

An entity that is using an external service provider has made clear agreements with the party to which it is outsourcing work.

The entity has maintained sufficient core competencies within its own organisation (in the form of expert compliance officers and auditors) to assess the implementation of the outsourcing of its CDD operations. The entity 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 entity also regularly evaluates the outsourcing to determine whether it is still working as intended, and whether it meets the legal requirements. Processes, systems and lists are assessed periodically.

GP2.11: Good practice - sharing confidential data

An entity sharing confidential data as part of an outsourcing arrangement can demonstrate that it requires the service provider with whom it shares that data to ensure confidentiality and information security at least at the same level as the entity itself.

The entity also applies the principle that information is only shared with this third party if this is necessary for the performance of the outsourced activities.

For more good practices, see the DNB guideline Good practices for managing outsourcing risks (dnb.nl).

2.3 Internal whistleblower scheme and DNB Integrity Reporting Desk

It is important that abuses in the financial sector are reported and investigated, as this contributes to both an ethical sector and financial stability. To ensure that this happens, the *Wwft* and the Whistleblower Protection Act (*Wet bescherming klokkenluiders – Wbk*) stipulate that entities must set up an internal reporting procedure for suspected wrongdoing within the organisation.[55]

As a competent authority, DNB also has a reporting procedure for suspected or confirmed wrongdoing at supervised entities.[56]

Q&A

QA.2.20: Question
At what size should an entity establish an internal reporting procedure for wrongdoing within the organisation?

Answer
The *Wwft* requires entities to have adequate facilities, appropriate to its nature and size, that allow their employees to report a breach of the *Wwft* internally and anonymously through a specific, independent channel.[57]

However, employers carrying out activities in the field of financial services are *always* required by law to set up a reporting channel and establish a procedure, regardless of the number of people they employ.[58] The reporting channel must comply with requirements as stipulated in the *Wbk*.

QA.2.21: Question
Who can report a breach of the *Wwft* or wrongdoing?

Answer
Any natural person who suspects wrongdoing in the context of their professional activities may report it. A person who files such a report is referred to as a whistleblower.

55 Section 20a(1) of the *Wwft*.
56 Section 20a(2) of the *Wwft*.
57 Section 20a(1) of the *Wwft*.
58 Section 2(3) of the *Wbk*.

QA.2.22: Question
an whistleblowers report wrongdoing to DNB?

Answer
Yes. Persons who suspect wrongdoing – including potential violations of the *Wwft* – at an entity supervised by DNB can submit a report to the DNB Integrity Reporting Desk.

More information on reporting wrongdoing can be found on the DNB website.[59]

QA.2.23: Question
Do I need to submit a report at my own organisation before I can report to DNB?

Answer
No, whistleblowers can report suspected wrongdoing directly to DNB.

Where appropriate, however, wrongdoing should first be reported internally at the institution, for example by using an internal whistleblower scheme.

QA.2.24: Question
What is the role of the Whistleblowers Authority?

Answer
The Whistleblowers Authority has several tasks, including providing advice to potential whistleblowers, investigating wrongdoing and assessing the treatment of whistleblowers.

For more information, please visit the Whistleblowers Authority's website.[60]

2.4 WTR2

Transfers of funds can be abused for terrorist financing and money laundering purposes. WTR2, which contains provisions about recording information on money transfers, aims to ensure that entities have insight into the origins and destinations of funds.[61]

Designated entities are required to share specific information with one another about the sender and beneficiary in the remittance chain. This information is vital to detecting terrorist financing and money laundering.

Q&A

QA.2.25: Question
What kind of money transfers does the WTR2 apply to?

Answer
The WTR2 applies to money transfers sent or received by payment service providers in the European Union, as well as to money transfers in which EU-based payment service providers act as intermediaries.[62]

59 For more information, go to https://www.dnb.nl/en/contact/reporting-complaints-and-wrongdoing/reporting-integrity-incidents-at-financial-entities/.
60 www.huisvoorklokkenluiders.nl.
61 Directive (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Directive (EC) No. 1781/2006, OJ 2015, L141/1, as subsequently amended.
62 Section 2 of the WTR2.

The WTR2 does not apply when money is transferred using credit or debit cards, electronic money instruments, or mobile phones or similar devices if these means of payment are used exclusively for the payment of goods or services. The number of the means of payment, however, must be included in all transfers resulting from the transaction in question.

QA.2.26: Question

To which part of the money transfer process does the WTR2 apply?

Answer

The WTR2 obligations primarily pertain to the recording of specific information about senders as well as beneficiaries throughout the chain. This means that the origin and destination of funds should be made transparent.

QA.2.27: Question

In a money transfer, what are the responsibilities of the sender's payment service provider on the one hand and the beneficiary's payment service provider on the other?

Answer

The WTR2 sets out the information that must be recorded when transferring funds:

- The sender's payment service provider must ensure that information is adequately recorded.[63]
- The beneficiary's payment service provider and (if applicable) the intermediatory payment service providers must check whether the information received is complete.[64]

If information is found to be incomplete, the entity should make a risk-based assessment to determine whether the transfer of funds should be refused, suspended or executed – and request the missing information.[65]

The Joint Guidelines of the European Supervisory Authorities (EBA, EIOPA and ESMA) provide further clarification.[66]

QA.2.28: Question

To what extent does the WTR2 apply to money transfers outside the EU?

Answer

The WTR2 applies to money transfers within the EU, regardless of currency.[67]

QA.2.29: Question

How should a payment service provider handle missing information on the sender or beneficiary?

Answer

The Joint Guidelines of the European Supervisory Authorities (EBA, EIOPA and ESMA) on the WTR2 describe how entities should handle money transfers involving missing information, as well as the procedures entities should put in place for this.

63 Section 4 of the WTR2.
64 Sections 7 and 11 of the WTR2.
65 Sections 8 and 12 of the WTR2.
66 EBA, ESMA & EIOPA, *Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information*, 2017.
67 Section 2(1) of the WTR2.

QA.2.30: Question
What is the relationship between the WTR2 and the upcoming Transfer of Funds Regulation (TFR)?

Answer
The WTR2 will be replaced by the TFR.[68] The TFR will take effect on 30 December 2024. There are two main differences between the WTR2 and the TFR:

- The TFR extends the requirements to crypto service providers falling within the scope of the Markets in Crypto Assets Regulation MiCAR.[69]
- With crypto transactions, the obligation to include information applies regardless of the size of the transaction. For transactions by payment service providers and credit entities, the regulation leaves room for Member States to apply a threshold of €1,000.

2.5 Protection of personal data

Natural persons have a fundamental right to the protection of their personal data during data processing.[70] Personal data collected under the *Wwft* is processed by entities for the purpose of preventing money laundering and terrorist financing and may not be further processed for commercial reasons or other reasons incompatible with that purpose.[71]

Q&A

QA.2.31: Question
Does the *Wwft*'s legal basis justify all forms of data processing by entities, as long as they serve the purpose of preventing money laundering and terrorist financing?

Answer
No, the existence of a legal basis does not justify every form of data processing. It is important that financial institutions continue to comply with the other requirements and principles of the General Data Protection Regulation (GDPR).[72] Data should only be processed if necessary, and the interests of the data subjects should be weighed against the interests of the controller.

Important principles are *proportionality* and *subsidiarity*. Any infringement of the right to privacy must be proportionate to the purpose (proportionality). In addition, there must be no other way to achieve the purpose for which the data is processed that is less detrimental to the data subjects (subsidiarity). Data processing is therefore unlawful if these principles and other GDPR requirements are not met.

68 Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets, repealing Regulation (EC) No. 1781/2006.
69 Regulation (EU) No. 2023/1114 of the European Parliament and of the Council of 31 May 2023 on crypto asset markets, amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
70 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Recital 1 of Directive 95/46/EC (the General Data Protection Regulation).
71 Section 34a(1) of the *Wwft*.
72 See also Grondslagen AVG uitgelegd | Autoriteit Persoonsgegevens.

QA.2.32: Question

Should customers be informed that their personal data is being processed?

Answer

Yes, entities must inform customers about their obligations under the *Wwft* and the related processing of personal data.[73] They must among others inform customers about the purposes for which their data is processed and the applicable legal retention period. It is important to note here that entities may not inform customers about reports made to FIU-NL (see QA4.27).

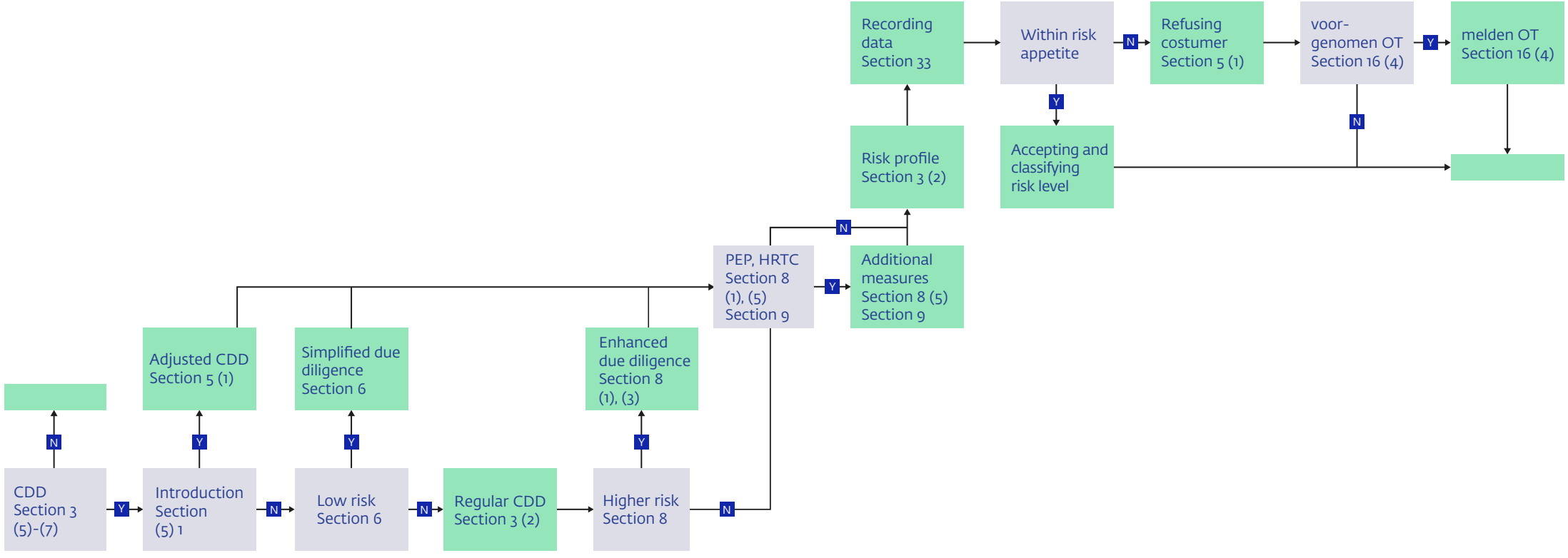
73 Section 34a(2) of the *Wwft*. 5.1a GDPR.

3 Customer due diligence: customer acceptance

This chapter discusses customer due diligence and customer acceptance as a possible outcome. Customer due diligence is mandatory under article 3 of the *Wwft*. Among other things, it enables the entity to identify and verify the identity of the customer and any UBOs, establish the purpose and intended nature of the business relationship, and to conduct ongoing monitoring. By extension, it allows the entity to make a risk assessment, on the basis of which it can determine whether regular customer due diligence procedure applies or simplified or enhanced due diligence.

Entities are – to a large extent – allowed to apply a risk-based approach to customer due diligence. Entities are – to a large extent – allowed to apply a risk-based approach to customer due diligence. It does however always need to be performed. Ultimately, the entity uses the information collected during the customer due diligence process to draw up a risk profile of the client. The entity has to record the collected information, and must assess whether to accept or reject the customer based on its risk tolerance.

The accompanying flowchart can be used as an aid when reading this chapter, and as a way of mapping out the various components of the customer due diligence process.


Recording data Section 33
Within risk appetite
N
Refusing costumer Section 5 (1)
voor-genomen OT Section 16 (4)
Y
melden OT Section 16 (4)
Y
Risk profile Section 3 (2)
Accepting and classifying risk level
N
N
PEP, HRTC Section 8 (1), (5) Section 9
Y
Additional measures Section 8 (5) Section 9
Adjusted CDD Section 5 (1)
Simplified due diligence Section 6
Enhanced due diligence Section 8 (1), (3)
N
Y
Y
Y
CDD Section 3 (5)-(7)
Y
Introduction Section (5) 1
N
Low risk Section 6
N
Regular CDD Section 3 (2)
Higher risk Section 8
N

3.1 Business relationship or relevant non-recurring transaction

By conducting customer due diligence, entities find out who they are doing business with. The nature of the investigation depends on the customer and the risks identified by the entity and is demonstrably tailored to these factors.[74]

Customer due diligence is required in at least the following cases:[75]

- when entering into a business relationship. A business relationship is a professional or commercial relationship between an entity and a natural person, legal entity or partnership firm, which is related to the professional activities of the entity and is expected to continue for a certain period from the moment the relationship is entered into.[76]
- in case there is no business relationship, when a non-recurring transaction of at least €15,000 is conducted on behalf of the customer, or multiple interrelated transactions totalling at least €15,000.[77]

In principle, customer due diligence should take place before the entity enters into a business relationship or performs a non-recurring transaction.[78]

GP3.1: Good practice - verifiably aligning customer due diligence in practice

- An entity has established an internal policy on how to conduct customer risk assessments. Risk assessments are carried out in accordance with this policy, and the results are recorded in the customer file. In carrying out the assessments, the entity takes into account the risks posed by the type of customer, business relationship, product or transaction.
- The compliance function must then check if customer due diligence has verifiably been aligned with the risk sensitivity to money laundering or terrorist financing of the type of customer, business relationship, product or transaction.

3.2 Introduced customer

Entities do not necessarily have to carry out their own customer due diligence but could also rely on the customer due diligence performed by another entity that is subject to the *Wwft*.[79] Both the accepting entity and the introducing entity have a responsibility for meeting their own customer due diligence obligations. This also applies to documenting the outcome of the investigation.

An entity may introduce a customer to another entity in the following situations:[80]

- An entity provides services for a customer who is already a customer of another institution.
- An entity introduces one of its own customers to another entity.

74 Section 3(8) of the *Wwft*.
75 Section 3(5) of the *Wwft*. See this article for the full overview of the cases wherein customer due diligence has to be performed.
76 Section 1(1) of the *Wwft*.
77 Legislative history shows that any individual money transfer (i.e. a transfer of money within the meaning of Directive (EU) 2015/2366) must be presumed to be indicative of a business relationship. See *Parliamentary Papers II*, 2007–2008, 31 238, no. 3, p. 12; *Parliamentary Papers II*, 2011–2012, 33 238, no. 3, p. 4.
78 Section 4(1) and Section 5(1) of the *Wwft*. Reasons for deviating from this guideline are described in Section 4 of the *Wwft* (e.g. see paragraph 3).
79 Section 5(1), under a Wwft, specifies which entities can introduce customers. If any other third party is involved Section 5 Wwft cannot be applied. Outsourcing as described in Section 10 Wwft can however possible be applied.
80 *Parliamentary Papers II*, 2007–2008, 31 238, no. 3, p. 23.

Q&A

QA3.1:Question
Can the accepting entity rely solely on confirmation from the introducing institution?

Answer
No, the accepting entity must be in possession of the introducing institution's customer due diligence data at the time of introduction.[81] In addition, the accepting entity must be in possession of the underlying documentation on which the customer's acceptance is based.

QA3.2:Question
When a customer is introduced, can the introducing institution's customer's risk profile be copied?

Answer
No, the accepting entity is responsible for preparing its own risk profile and must have the right data to do so.

QA3.3:Question
What if the introducing entity is unable to provide the customer's details?

Answer
If the introducing entity cannot provide the required information, the accepting entity will conduct the customer due diligence necessary pursuant to the *Wwft*.

QA3.4:Question
When a customer is introduced, must the customer consent to their personal data being shared with another institution?

Answer
Yes, pursuant to Section 6 of the General Data Protection Regulation (GDPR), consent must be sought from the customer. Although the so-called "principle of purpose" is in fact regulated by Section 34a of the *Wwft*, the customer's personal data is shared with another processor when they are introduced.

GP3.2: Good practice - intermediary assessment

In its customer identification and verification policy, a life insurer lays down how it assesses intermediaries to ensure that they can be relied on to perform identification and verification. It also lays down how, when and for what reasons the intermediaries must share customer identification and verification data.

GP3.3: Good practice - assessment of the introducing institution's procedures and measures

An entity uses a risk-based approach to verify that introducing entities have adequate customer due diligence processes in place. For example, it asks entities that introduce more than 50 customers per year on average to submit their *Wwft* procedures for review. For entities that introduce more than 100 customers per year on average, an accountant's report on the effectiveness of the *Wwft* procedures is also requested. At other entities, the entity performs spot checks.

81 Section 33(1) of the *Wwft*.

3.3 Simplified customer due diligence

The *Wwft* stipulates a risk-based approach. Based on this approach, a risk assessment may also conclude that an entity can suffice with simplified customer due diligence, for instance if the nature of a business relationship or transaction is correlated with a low risk of money laundering or terrorist financing.[82]

An entity must have enough information about customers for which it uses simplified customer due diligence to ensure that a simplified process suffices and that it is able to comply with its obligation to report unusual transactions.[83]

Q&A

QA3.5: Question
What does simplified customer due diligence entail?

Answer
The law does not specify what constitutes simplified customer due diligence. The intensity of customer due diligence can be tailored to the risk level.[84]
In case of simplified customer due diligence must the obligations of Section 33(2) *Wwft* must still be met. The entity also has to meet the reporting obligations of Section 16 Wwft.

QA3.6: Question
Should customer due diligence always be applied?

Answer
Yes, customer due diligence always needs to be applied. Even in case the risk so low that simplified due diligence can be performed.[85]

QA3.7: Question
Should an entity always carry out a risk assessment in case of a potential low risk?

Answer
Yes, the conclusion that simplified customer due diligence is appropriate must always be based on a risk assessment. This means that a risk assessment must always be carried out so that the intensity of the customer due diligence process can be tailored to the assessed risk.

QA3.8: Question
What factors indicate that a customer may be low risk?

Answer
In its risk assessment, the entity must at least include the non-exhaustive list of risk factors in Annex II of the Fourth Anti-Money Laundering Directive.[86] These factors can give a first indication that a customer may be low risk. For example, the involvement of government agencies, both in EU Member

82 Section 6(1) of the *Wwft*.
83 Section 6(2) and (4) in conjunction with Section 16(2) of the *Wwft*.
84 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 9.
85 Section 5(4) of the Wwft.
86 Section 6(1) of the *Wwft*.

States and third countries that have effective anti-money laundering and terrorist financing legislation and oversight, may indicate low risk.

Further risk factors are also listed in the EBA "ML/TF Risk Factors Guidelines".[87]

QA3.9: Question
Are listed customers always low risk?

Answer
No, a stock market listing may be a risk-mitigating factor, but entities cannot simply assume that a listed customer always carries lower risk. Other customer-related risk factors may also play a role, such as where the entity is listed and what percentage of its share capital is marketable. With regard to the location of listing, for example, EU transparency rules (and other similar rules) provide insight into the ownership of shares, which is not necessarily the case in other countries. In addition, there may also be non-customer-related risk factors at play, for instance with regard to the type of product, service or transaction. These may also include geographical risk factors.

In order to estimate the degree of depth with which customer due diligence should be carried out, it is necessary to first perform a risk analysis.

QA3.10: Question
Are customers that are subject to the *Wwft* themselves always low risk?

Answer
If a customer is subject to the *Wwft*, this may be a risk-mitigating factor. However, it does not automatically indicate a lower risk of money laundering or terrorist financing.[88] An entity may consider this factor in its risk assessment of a business relationship or non-recurring transaction.

GP3.4: Good practice - using risk factors

An entity estimates in advance for which customers it will be able to use simplified customer due diligence. This is done through a preliminary risk analysis that takes into account relevant risk factors. The entity includes customer-related risk factors as well as product-, service-, transaction- and delivery channel-related and geographical risk factors in this risk analysis. The entity regularly updates its risk analysis based on the latest insights from incidents, FIU reports, sector-wide developments, etc.

The entity substantiates that the business relationship or transaction in question, by its nature, carries a lower risk of money laundering or terrorist financing, and documents this.

87 EBA, *Guidelines on ML/TF Risk Factors*, 2021.
88 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 35.

GP3.5: Good practice - aligning intensity of measures with risk level

An entity uses a simplified customer due diligence process for certain low-risk customers, based on its risk analysis. By extension, measures in the context of continuous monitoring of business relationships are also applied less intensely. The entity monitors these customers through transaction monitoring and sanctions screening using reference groups. If a customer's transaction behaviour differs from the peer group, this is reason for the entity to review the customer relationship and request additional information if necessary. As long as there is no abnormal behaviour, the entity does not review the customer relationship.

GP3.6: Good practice - establishing low risk

An insurer considers a term life insurance policy with an annual premium of less than €2,500 to be low risk, and has determined that factors such as the delivery channel, type of customer and geographical location do not adversely affect risk. The insurer therefore uses a simplified customer due diligence process for this category.

3.4 Standard customer due diligence

3.4.1 Customer identification and identity verification

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

For identification purposes, the customer must submit proof of identity. There are no strict rules for the form thereof; the aim of the verification process is to determine whether the proof of identity submitted matches the customer's real identity. The entity must verify the authenticity of the proof of identity submitted by the customer on the basis of documents, data or information from credible and independent sources.

The identity of any representatives of the customer should also be verified (also see paragraph 3.4.3.).

Q&A

QA3.11: Question

How should a customer's identity be verified?

Answer

A customer's identity must be verified on the basis of documents, data or intelligence from reliable and independent sources.[89]

Section 4 of the Decree implementing the Anti-Money Laundering and Anti-Terrorist Financing Act 2018 (*Uitvoeringsregeling Wwft 2018*) provides a list of documents that can be used to verify a customer's identity. This overview is not exhaustive. Furthermore, the obligations of Section 33 Wwft need to be met. More generally, documents cannot be used to verify a customer's identity if it is not possible to confirm that they have been preceded by adequate identification and verification. This includes student IDs, employee badges and statements from utility or phone companies.

89 Section 11 of the Wwft.

QA3.12: Question
Can electronic identification (eID) be used for identity verification of the customer?

Answer
Yes, eID tools can be used for identity verification if they are sufficiently reliable. An eID tool is sufficiently reliable if its assurance level is "substantial" or "high". These assurance levels are defined in the eIDAS Regulation.[90]

QA3.13: Question
Does a name-number check qualify as identity verification of the customer?

Answer
As a rule, a name-number check, for example by transferring 1 cent, is not sufficient for identity verification. This means that one or more other independent and reliable sources must be used in addition to a name-number check.

GP3.7: Good practice - establishing the reliability of sources

An entity has defined which documents, information or data are acceptable for the purpose of customer identity verification, and why. The entity has also looked at common practices in international money transfers.

To verify a customer's identity, it carries out a risk assessment, taking into account the European Commission's list of high-risk countries. This risk assessment shows that the entity understands which sources are reliable and independent. The entity 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.

3.4.2 Ultimate beneficial owner (UBO) & pseudo-UBO

The ultimate beneficial owner (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.[91] 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 entities know who they are dealing with, that they have insight into the ownership and control structures of their customers, and that they know who manages their customers and ultimately benefits from the services they provide.

90 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 and repealing Directive 1999/93/EC
91 Section 1(1), under b, of the *Wwft*.

Q&A

QA3.14: Question
Should a UBO be identified for each legal entity?

Answer
Yes. The *Wwft* stipulates that entities must identify the ultimate beneficial owners (UBOs) of customers and take reasonable measures to verify their identity, with the exception of publicly traded companies to which transparency requirements[92] already apply, including 100% subsidiaries of those companies.[93]

UBOs are always natural persons. The standard set out in the *Wwft* is not only relevant when the customer is a legal entity, such as a private limited liability company or a foundation, or a legal structure, such as a trust, but also when the customer is a natural person controlled by another natural person or on whose behalf a transaction or activity is carried out.

QA3.15: Question
In what cases is insight into the customer's ownership and control structure required?

Answer
An entity must take reasonable steps to gain an understanding of the ownership and control structure of the customer in the case of legal entities and other legal structures, such as trusts.[94] This includes measures to verify the legal status of customers other than natural persons, if possible by obtaining proof of incorporation.[95]

The goal is that the entity knows and understands the structure of the customer. The depth of the investigation should match the complexity of the structure and the risk.

QA3.16: Question
When does a natural person qualify as a UBO?

Answer
Section 3 of the Decree implementing the Anti-Money Laundering and Anti-Terrorist Financing Act 2018 (*Uitvoeringsbesluit Wwft 2018*) elaborates on natural persons who must in any case be considered UBOs. It also sets out how UBOs should be identified for different types of legal entities. The implementation decree includes rules for public and private limited companies,[96] religious

92 This means the transparency requirements as part of Directive 2004/109/EC of the European Parliament and of the Council of 15 December 2004 on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market and amending Directive 2001/34/EC, or equivalent transparency *requirements of a country* located outside the EU.
93 Section 3(1), under a, of the Wwft implementing decree.
94 Section 3(2), under b, of the *Wwft implementing decree*.
95 Basel Committee on Banking Supervision, *Guidelines on the Sound Management of Risks Related to Money Laundering and Terrorist Financing*, 2020, Annex 4.
96 Section 3(1), under a, of the *Wwft implementing decree*.

organisations,[97] other legal entities (including foundations and associations)[98] and partnership firms (including general partnerships).[99]

For most legal entities, under the implementation decree, a natural person qualifies as a UBO if they directly or indirectly have more than 25% ownership in or control over the legal entity. For example: in the case of private and public limited companies, UBOs are the individuals who ultimately own or control the company by directly or indirectly holding more than 25% of the company's shares, voting rights or ownership interest.

The 25% rule is meant to be indicative.[100] Individuals with smaller interests may also qualify as UBOs if they otherwise have ultimate control or ownership.

If, after exhausting all possible means, and there are no grounds for suspicion, no UBOs have been identified or if there is doubt that these persons are the UBOs, , then the persons of the legal entity's senior management will be considered UBOs.[101]

QA3.17: Question
Should identity documents be requested in all cases to meet the verification requirement?

Answer
No, this is not always necessary. An entity must take reasonable measures to verify the UBOs' identity. For example, if a simplified customer due diligence process is used, it may suffice to have the customer declare that the UBOs' listed in the Trade Register are in fact its UBOs, and that their stated identity matches their actual identity. Entities should in any case take into account the appropriateness of the measures taken (also see QA3.18).

QA3.18: Question
What are "reasonable measures" to verify a UBO's identity?

Answer
"Reasonable measures" are measures which are commensurate to the risk level. Although the Wwft does not dictate which information sources are sufficient for verifying the UBO's, the used sources have to be sufficient for achieving the intended purpose. The point is that the entity must know who the UBO is, and that it must have sufficient reliable information about their identity, appropriate to the risk level.

QA3.19: Question
What if no UBOs can be identified or if there is doubt about a UBO?

Answer
An entity is held to refuse or terminate the provision of services in case no UBO can be determined. In that case the requirements of customer due diligence cannot be met.[102] In cases where no UBO can be determined on the basis of ownership or control, there is the fallback-option of the pseudo-UBO: the natural persons who make up the customer's senior management are in that case considered

97 Section 3(1), under b, of the *Wwft implementing decree.*
98 Section 3(1), under c, of the *Wwft implementing decree.*
99 Section 3(1), under d, *Wwft implementing decree.*
100 *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 4.
101Section 3(1) of the *Wwft implementing decree.*
102 *Government Gazette* No. 241, p. 29 on the *Wwft implementing decree.*

pseudo-UBOs, provided certain conditions are met. This is further elaborated in Section 3 of the Decree implementing the Anti-Money Laundering and Anti-Terrorist Financing Act 2018 (*Uitvoeringsbesluit Wwft 2018*).

Senior executives can only be identified as pseudo-UBOs if the entity has exhausted all possible methods of identifying a customer's UBOs, and if there are no grounds for suspicion of money laundering or terrorist financing. The entity must document the measures it has taken and any difficulties encountered during the verification process.[103]

GP3.8: Good practice - investigating customer's role in complex structure

A legal entity seeking to become a customer of an entity is part of a larger structure. The parent of this legal entity, which is based in a country outside the EU, also has subsidiaries in high-risk countries.

The entity investigates why the group to which the customer belongs uses this complex structure. It also questions the customer about the rationale behind this structure, and about how it functions. Moreover, the entity requires the customer to provide a legal and/or tax opinion about the functioning of the structure.

After the entity has examined the opinion(s) submitted by the customer, it finishes its investigation, determining that it still does not understand the customer's role in the structure. The entity concludes that the customer due diligence process cannot be properly completed and therefore decides not to accept the customer.

GP3.9: Good practice - simple structures

A partnership firm operating a butchery has two shareholders who are also the company's directors, as shown by the Trade Register of the Chamber of Commerce and a conformation of that information by the customers. The shareholders are brothers. The entity has sufficient understanding of customer's ownership and control structure and designates the brothers as UBOs.

GP3.10: Good practice - identifying UBOs based on level of control

Customer due diligence reveals that a customer has a major financier. This person is not a shareholder in the company and has no voting rights, but they do have the right to veto important decisions. The entity designates this person as a UBO by virtue of their level control, in addition to the director/majority shareholder already identified.

GP3.11: Good practice - risk-based approach

For a low-risk customer, an entity has requested a copy of the UBO register, which it submits to the customer for verification. 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 entity has no reason to question this. This completes the identification and verification process.
For a high-risk customer, the entity takes additional measures to verify the identity of the UBOs, for example by requesting certified copies of identity documents or by means of sufficiently reliable electronic identification.

103 Section 3(2), under b, of the *Wwft*.

GP3.12: Good practice - identifying pseudo-UBOs for low-risk customers

An entity has determined that a customer is low risk. The entity cannot identify a UBO based on the company's ownership and control structure, and therefore identifies the senior executives of the customer as pseudo-UBOs. To substantiate this, it submits a list of the company's senior management personnel retrieved from the Trade Register to the customer. The customer confirms that the persons listed are in fact its senior executives and that their stated identity matches their actual identity. The entity has no reason to doubt this. This completes the identification and verification process. The entity documents the measures it has taken and the difficulties it encountered during the verification process.

GP3.13: Good practice - identifying pseudo-UBOs for high-risk customers

An entity has determined that a customer is high risk, but there are no grounds for suspicion of money laundering or terrorist financing.

The entity cannot identify a UBO based on the company's ownership and control structure, and therefore identifies pseudo-UBOs based on data from the Trade Register. The entity additionally requests that the customer provide a list of its senior management personnel. The identity of these natural persons is verified on the basis of identity documents. The entity documents the measures it has taken and the difficulties it encountered during the verification process.

GP3.14: Good practice - adding up interests

An entity has a customer that is part of a larger structure. The entity determines that none of the direct shareholders hold more than 25% of the shares. When it investigates the company's structure, however, the entity identifies a number of individuals who have several interests through multiple companies. After adding these up, the entity determines that there are two natural persons with a total interest of more than 25%. The entity identifies these individuals as UBOs.

GP3.15: Good practice - investigating UBOs

A customer has an elaborate, multi-layered company structure. Some of its shareholders are based in high-risk jurisdictions. Given the risks identified for this customer relationship, the entity does not accept the customer's self-reported list of UBOs as sufficient evidence. The entity takes reasonable measures to map the company's ownership structure (for example using extracts from the Trade Register and additional sources) and identifies three individuals as UBOs. These individuals each have indirect formal control of more than 25%. The entity then verifies the identity of these UBOs through certified copies of identity documents. It documents its findings (the sources, analysis and conclusions) in the customer file.

GP3.16: Good practice - screening minority shareholders for high-risk customers

A customer is classified as high risk based on several risk factors, including risks related to the company's ownership and control structure. The entity subsequently decides to conduct enhanced customer due diligence, and as such investigates the control exercised by shareholders with an ownership share of less than 25% are present in the structure. Based on that research the entity concludes that, in line with its own policy, certain shareholders with a smaller ownership percentage are also UBOs. It also applies PEP screening these shareholders.

GP3.17: Good practice - policy on handling complex structures

An entity that predominantly deals with complex international ownership and control structures has established policies setting out when an internal or external expert opinion (for instance from a tax specialist) should be sought regarding a customer's structure.

GP3.18: Good practice - policy on identifying and verifying UBOs of EU customers

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

- For low- and neutral-risk customers, a UBO's identity can be verified on the basis of a statement from the local 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.

3.4.3 Representation and "straw man risk"

A natural person can act as a representative of a customer. The *Wwft* stipulates that the entity must verify that this person is authorised to represent the customer.[104] If this is the case, the entity can proceed with its customer due diligence process.

Furthermore, it is important to determine whether a natural person presenting as a customer acts on their own behalf or for another.[105] This determines whom can be considered the customer.

Q&A

QA3.20: Question

Should the entity verify whether the representative is authorised?

Answer

During the customer due diligence process, the entity verifies that the natural person acting as the customer's representative is authorised to represent the customer.[106] This applies for example in situations in which a natural person acts as a legal entity's director.[107]

QA3.21: Question

Can a natural person have a representative as well?

Answer

Yes, a natural person can also have a representative.

QA3.22: Question

To what extent should the entity identify the representative and verify their identity?

Answer

The service provider should identify the natural person and verify its identity.[108]

104 Section 3(2), under e Wwft
105 Section 3(2), under f of the Wwft.
106 Section 3(2), under e of the Wwft.
107 *Parliamentary Papers II*, 2011–2012, 33 238, no. 3, p. 12
108 Section 3(2), under e of the Wwft

QA3.23: Question What do entities need to be extra vigilant about?

Answer
During the customer due diligence process, the entity must determine whether a person presenting as a customer is acting on their own behalf, or on behalf of someone else.[109] This also allows the entity to check whether someone is being used as a so-called straw man, acting on behalf of criminal third parties.

If it is clear that someone is acting on behalf of another person, this other person should be seen as the customer and subjected to customer due diligence.

QA3.24: Question
Should the entity check whether someone is being used as a straw man?

Answer
The Wwft obligates entities to take reasonable measures to determine whether the customer acts on its own behalf of for another.[110] Entities can use a risk-based approach and concentrate their efforts on cases where there appears to be an increased "straw man risk".

GP3.19: 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 and the articles of association of the entity.

GP3.20: Good practice - straw man risk indicators

An entity establishes indicators of "straw man risk" and applies these in the customer due diligence process. Indicators may include instances where a person is unable to answer certain questions, for example about the origin of the funds, or where unclear, vague reasons are given for the transaction.
If the entity suspects that the customer is a straw man, this is treated as an increased or unacceptable risk. If it is clear that a customer is acting on behalf of another natural or legal person, the entity treats this other person also as the customer, meaning that the customer due diligence obligations also apply to this person.

3.4.4 Purpose and intended nature of the business relationship

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

109 Section 3(2), under f of the Wwft
110 Section 3(2), under f, of the *Wwft*.

Q&A

QA3.25: Question
Should an entity always establish the purpose and intended nature of the business relationship?

Answer
Yes, it should. The *Wwft* states that customer due diligence should enable the entity to establish the purpose and intended nature of the business relationship.[111] The entity must tailor the intensity of the investigation to the risk of money laundering and terrorist financing.

QA3.26: Question
To what extent can the purpose and intended nature of the business relationship be established based on the products purchased?

Answer
Establishing the purpose and intended nature of the business relationship enables an entity to estimate the risk involved in providing services to a customer.

The information required for this will usually become available as a result of contact prior to the business relationship.

The purpose and intended nature of the business relationship may – taking into account the characteristics of the customer – be evident from the services or products purchased by the customer. These may include:

- a current account for regular payment transactions (private/business account);
- life insurance products;
- traditional investment products for wealth protection/asset accumulation;
- a securities account.

If the purpose and intended nature of the business relationship are not apparent based on the services and/or products purchased by the customer, additional information must be collected.

QA3.27: Question
Can the purpose and intended nature of the business relationship be established using peer grouping?

Answer
Yes, it can. The purpose and intended nature of the business relationship must be determined with a view to assessing the risk level involved. An entity may classify its business relationships into peer groups. For specific peer groups nature and purpose of the business relationship could be sufficiently clear.

GP3.21: Good practice - questioning customers in case of doubt

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

111 Section 3(2), under c, of the Wwft

GP3.22: Good practice - increased scrutiny for high-risk customers

Customers may also be high risk because they are domiciled, established or have their registered office in a high-risk country, due to the involvement of a PEP or because there is a correspondent relationship.

If this is the case, the entity must determine what kind of transactions the customer will carry out by examining the expected nature, quantity, frequency and size of the transactions, and the countries or territories the customer will likely transact with. This contributes to determining the nature of the relationship. On the basis of this assessment, the entity must create a risk profile and determine whether, and under what conditions, the risk level is acceptable.

GP3.23: Good practice - use of peer groups

An entity with a large number of customers uses peer groups. The entity has defined peer groups based on a number of customer characteristics. For customers who do not fall into a peer group, the entity obtains further information on the purpose and intended nature of the business relationship, among other things, while also gaining a better understanding of what kind of transactions the customer intends to carry out.

GP3.24: Good practice - collecting additional information

If a customer is considered high risk, the entity collects additional information (for instance on the type of transactions the customer intends to conduct, the volume thereof and the activities of the customer). Partly on the basis of this information, the entity then establishes the purpose and intended nature of the relationship.

3.4.5 Source of funds

Establishing the business relationship's source of funds used in the business relationship or transaction strengthens the insight that the entity has in the risks of providing services for the customer. This includes amongst others the risk that the entity facilitates criminal money flows.

Q&A

QA3.28: Question

Should an entity always establish the source of funds?

Answer

No. The entity should only when necessary conduct an investigation into the source of funds used in the business relationship or transactions performed in the course of the business relationship. Whether this is necessary,[112] depends on the risk assessment performed by the entity.[113]

The *Wwft* prescribes that the source of funds must always be investigated in the following two situations:

- In case of transactions, business relationships and correspondent relationships involving states identified by the European Commission as higher-risk jurisdictions for money laundering and terrorist financing. Entities must then collect information on the source of the funds used in the business relationship or transaction, and on the source of the customer's and UBOs' assets.[114] This requirement can be met using a risk-based approach.[115]
- In addition, when entering into or continuing a business relationship with, or conducting a transaction for, a PEP, entities must take appropriate measures to determine the source of the PEP's assets, and of the funds used.[116]

112 Section 3(2), under d, of the *Wwft*.
113 *Parliamentary Papers II*, 2011–2012, 33 238, no. 3, p. 12.
114 Section 9(1), under c, of the *Wwft*.
115 *Parliamentary Papers II*, 2018–2019, 35 245, no. 3, p. 30. EBA (2021) *Guidelines on ML/TF Risk Factors*, Sections 4.53 and 4.54.
116 Section 8(5), under b(2), of the *Wwft*.

QA3.29: Question
Should the entity investigate the source of funds if the funds come from a regulated institution?

Answer
The fact that the funds originate from a regulated entity may be a risk-mitigating factor, but this does not mean that the receiving entity is exempted from performing a due diligence review. Depending on the risks identified, the entity must determine whether investigation into the source of the funds is needed.[117]

QA3.30: Question
To what extent should the origin of all the customer's assets be investigated?

Answer
Usually, the entity only needs to investigate the resources used in the business relationship or transaction.[118] This means that the rest of the customer's assets can be disregarded. Depending on the risk level, however, a more comprehensive investigation into the origin of the customer's assets may be warranted.

In the case of customers and UBOs that qualify as PEPs, or that are related to states designated by the European Commission as having a higher risk of money laundering or terrorist financing, entities must take appropriate measures to identify the sources of funds and wealth, or gather the information on the origins of the funds or wealth.[119]

GP3.25: Good practice - use of indicators for depth of research
To determine the likelihood that funds originate from a lawful source, the entity should identify specific indicators to determine the depth of the research. Examples of such indicators include the amount concerned, the stated explanation for the origin of the funds, the customer's age and occupation or business activities, the country of origin or destination of the funds, and the product or service provided.

GP3.26: Good practice - research policy and documentation
For large deposits that fall outside the customer's risk profile, an entity investigates the source of the funds. In addition, all customers classified as high risk are subject to investigation into the source of their funds based on independent, reliable sources. The entity documents the investigation process, evidence and conclusion in the customer file.

GP3.27: Good practice - documentary evidence on source of funds
When investigating the source of a customer's funds, an entity uses independent, reliable sources. Depending on the risk level, the entity uses certified copies of payslips, employer statements, a sales contract, overviews of share positions, wills, annual accounts, tax returns and other documents.

117 See Section 3(8) and (9) of the Wwft and Annex I to the Fourth Anti-Money Laundering Directive on tailoring customer due diligence to ML/TF risk sensitivity based on various factors.
118 *Parliamentary Papers II*, 2011–2012, 33 238, no. 3, p. 12.
119 Section 8(5), under b(2), of the *Wwft*. Section 9(1), under c, of the *Wwft*. See also *Parliamentary Papers II*, 2017–2018, 34 808, no. 3, p. 55-56.

GP3.28: Good practice - rent payments

A customer wants to open a business account with a bank and use it to receive rent payments. Inquiries reveal that the customer owns a number of office properties, which he rents out.

As part of the investigation into the source of funds, the bank wants to know whether the ownership of the office properties fits the customer's background. It investigates the origin of the customer's assets in order to better understand the source of the funds coming into the bank.

3.5 Dealing with politically exposed persons (PEPs)

A PEP is a person who holds or has held a prominent public position. Because of the potential corruption and reputation risks associated with PEPs, the *Wwft* requires entities to pay special attention to these individuals.[120]

PEPs do not automatically carry a high risk of money laundering or terrorist financing.[121] Risk-increasing factors that may be associated with PEPs include access to large public funds, control over state-owned companies and contracts, and opportunities to channel public money into structures created by the PEP themselves.[122].

It is therefore important for entities to know whether their customer or the customer's UBO is a PEP. With this knowledge, the entity is better able to assess the customer's risk level.

Q&A

QA3.31: Question
Who qualifies as a PEP?

Answer
A PEP is defined as a natural person who holds or has held a prominent public position. PEPs also include family members or close associates of that person.[123]

Section 2(1) of the Decree implementing the Anti-Money Laundering and Anti-Terrorist Financing Act 2018 (*Uitvoeringsbesluit Wwft 2018*) details what is considered a prominent public position, as well as who are considered family members and close associates.[124]

QA3.32: Question
Do all PEPs pose a high risk?

Answer
No. Although the Wwft assumes PEPs carries an increased risk, a PEP is not necessarily high risk. This depends on more factors than just PEP status.[125]

For instance, children of a Dutch member of parliament with a basic payment account are potentially less risk-prone than the spouse of a head of state of a country with an increased risk of corruption who opens a private bank account.

120 *Parliamentary Papers II*, 2007–2008, 31 238, no. 3, p. 21-22
121 FATF, *Specific Risk Factors in Laundering the Proceeds of Corruption: Assistance to Reporting Institutions*, 2012, p. 4.
122 FATF, *FATF Report Laundering the Proceeds of Corruption*, 2011.
123 Section 1(1) of the *Wwft*.
124 The Tax and Customs Administration has published a list of prominent public positions based on Section 2 of the Decree implementing the Anti-Money Laundering and Anti-Terrorist Financing Act 2018 (*Uitvoeringsbesluit Wwft 2018*). See https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/wwft-prominente-publieke-functies.
125 FATF, *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)*, 2013. It may be useful in this context to be aware of the level of corruption in the individual's country of origin, for example by referring to Transparency International's Corruption Perceptions Index.

QA3.33: Question
What additional measures are mandatory in relation to PEPs?

Answer
The following additional measures are mandatory in dealing with PEPs:[126]

- A senior executive at the entity must approve decisions to enter into or continue a business relationship with a PEP or execute a transaction for a PEP.[127]
- Entities must take appropriate measures to identify the source of assets and funds used in the business relationship or transaction.
- The business relationship must be subject to ongoing enhanced due diligence.

Entities can tailor the intensity of the measures and the depth of the research to be carried out to the risk profile of the customer or UBO. The additional measures can however not be wholly omitted.

QA3.34: Question
Does someone's PEP status expire when they no longer qualify as a PEP?

Answer
If the customer or the UBO ceases to hold a politically exposed position, the entity must continue to apply appropriate risk-based measures as long as necessary, and at least during the next 12 months, until the heightened risk associated with politically exposed persons no longer applies to the person involved.[128]

QA3.35: Question
What if an existing customer becomes or is found to be a PEP?

Answer
If an existing customer or UBO becomes or is found to be a PEP (or a family member or close associate), the entity must take the required measures without delay as soon as this becomes apparent.[129]

GP3.29: Good practice - PEP screening

Entities must assess whether customers and their UBOs qualify as PEPs during onboarding. They must also perform regular checks for existing customers and UBOs. Entities must combine this PEP check with other ongoing screenings, including monitoring for any negative media attention. If it appears that an existing customer or UBO qualifies as a PEP, the entity will first assess the risk level. It then takes measures applicable and appropriate to the PEP.

126 Section 8(5) of the *Wwft*.
127 Section 1(1) of the Wwft: senior management: a. the persons that determine the daily policy of the entity; or b. those persons working under the responsibility of an entity, that have a leadership position directly below the persons that determine the daily policy of the entity which are responsible for natural persons whose tasks influence the exposure of an entity to money laundering and terrorist financing risks.
128 Section 8(7) of the *Wwft*.
129 Section 8(9) of the *Wwft*.

GP3.30: Good practice - multiple methods to determine PEP status

An entity uses the following methods to investigate whether a person qualifies as a PEP:

- Screening against available PEP lists.
- In addition to using general PEP lists, the entity also screens against its own "local" PEP lists, running a check on names of local individuals in prominent positions.
- Conducting internet research, for example consulting the trade register in the customer's country of origin to collect information about the company's management.
- To gather sufficient information to identify PEPs during the CDD process, and to find out if there are any family members or close associates who qualify as PEPs, the entity uses a targeted questionnaire.

GP3.31: Good practice - PEPs and complex structures

An entity knows that just running a check against a PEP list does not suffice in every situation. It is aware that PEPs may hide behind another person (concealment or straw man risk). If a customer is part of a complex structure, the entity makes additional efforts to understand this structure and identify the UBO. In doing so, the entity focuses not only on 'ownership' but also on 'control.'

The compliance function performs targeted checks on the operation and effectiveness of procedures for identifying PEPs.

GP3.32: Good practice - up-to-date PEP lists

An entity periodically checks whether all relevant lists for the PEP-screening are used and up to date. To keep the PEP lists it uses up to date, it has a subscription with an external service provider. The entity updates its local PEP list after significant events, such as elections and board changes.

GP3.33: Good practice - use of red flags

In conducting PEP risk assessments, an entity uses a number of risk indicators, or red flags. The entity considers the risk higher in the following cases:

- The PEP is from a jurisdiction with a higher risk of money laundering and/or corruption, or from an EU- or UN-sanctioned country.
- There is negative news about the PEP, or the PEP has a troubled legal history.
- Available information on the customer (occupation, age, income) does not wholly match the information on source of funds and assets.
- The customer/UBO provides documents on the source of their funds and wealth that are inconsistent with those provided by comparable customers.
- The customer/UBO provides documents on the source of their funds and wealth originating from high-risk jurisdictions.
- The customer/UBO provides documents on the source of their funds and wealth that are inadequate or lack rationale.
- The customer/UBO provides information on the source of their funds and wealth through complex, opaque structures (e.g. offshore structures, trusts, bank accounts in high-risk countries), and the information remains unclear.

The entity must take additional management measures in these situations, such as asking additional questions, setting limits on transaction amounts and pre-assessing transactions the PEP wants to conduct. The entity must also consider whether the risk is still acceptable and whether customer due diligence can be properly completed. If not, the entity should refuse, terminate or limit its services.

GP3.34: Good practice - eye for the customer

An entity uses a risk-based approach for its enhanced customer due diligence, keeping in mind the potential burden on the customer and the employee tasked with carrying out the investigation. The entity also acknowledges the possibility of resistance from the customer or employee if they do not understand why certain information has to be provided. The entity therefore clearly explains why certain information is requested, both externally to its customers and internally to its employees.

GP3.35: Good practice - involving senior executives

An entity's senior executives not only play a role in approving business relationships and transactions, but they are also regularly informed about PEP exposure and sign off on it.

Furthermore, the compliance function actively monitors the acceptance of customers when a PEP is involved and provides an opinion about acceptance. It considers the total "PEP exposure" and the actual risk the entity may face upon acceptance, and it has the resources and position to operate and advise independently in these matters. The compliance function's opinion on the risk level plays an important role in senior management's decision on the relationship.

3.6 Dealing with high-risk countries

The FATF and the European Commission regularly identify jurisdictions that have weaknesses in their anti-money laundering and counter-terrorist financing systems. Maintaining business relationships with residents of such jurisdictions, or conducting transactions to or from these jurisdictions, may involve an increased risk of money laundering and terrorist financing. It is therefore important that entities be extra vigilant with regard to business relationships and transactions related to high-risk countries (also known as high-risk third countries (HRTCs), including the execution of enhanced due diligence.[130]

Q&A

QA3.36: Question
Which countries are considered high risk for money laundering and terrorist financing by the European Commission?

Answer
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 (high-risk third countries (HRTCs)).[131]

These countries are listed in the Commission Delegated Regulation (EU) 2016/1675 supplementing European Parliament and Council Directive (EU) 2015/849. This list is updated regularly.

130 Section 8(1) under b and Section 9 of the *Wwft*.
131 Section 9(1) of the *Wwft*.

QA3.37: Question
Should an entity be extra vigilant in relation to every transaction involving an HRTC?

Answer
Section 9 of the *Wwft* requires entities to carry out a number of enhanced investigative measures with respect to transactions, business relationships and correspondent banking relationships involving HRTCs. The intensity of these measures may vary on a case-by-case basis depending on the risk level, for example with regard to the collection of additional information.

In any case, entities are expected to be able to explain their reasoning as to why a lower level of scrutiny was applied in a particular case.

QA3.38: Question
What measures should an entity apply to business relationships and transactions involving an HRTC?

Answer
Section 9(1) of the *Wwft* lists the enhanced investigative measures. This includes gathering background information on the customer's intended or completed transactions and obtaining approval from senior management for entering into or continuing the business relationship.

QA3.39: Question
In transactions involving HRTCs, should entities always approach the customer directly to collect additional information?

Answer
No. Using a risk-based approach, an entity may, in certain cases, collect additional information through its own desk research or from public sources, without directly contacting the customer.

For instance, information in the customer file on the customer's identity and the source of funds does not need to be requested again if it is up to date, unless a situation occurs that does not fit the customer's profile.

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

In short: the entity should only question the customer if this is necessary given the risk level and the institution's pre-existing information position. However, the entity must always be able to substantiate why it chose to apply a lower level of scrutiny and document its decision-making process.

QA3.40: Question
What should an entity do when the European Commission updates its HRTC list?

Answer
Enhanced investigative measures must be used from the moment a country is added to the list. From then on, the entity must apply these measures as per Section 9 of the *Wwft*.

If a country is removed from the list by the European Commission, the enhanced screening measures no longer need to be applied.

QA3.41: Question
Should senior executives approve each individual transaction involving an HRTC?

Answer
The point is that entities should not enter into or decide to continue a business relationship without approval from senior management.

Individual transactions, however, do not need to be approved by senior management. The relevant requirement in the law refers to business relationships, not transactions. Approval by senior management should therefore be given at the time of entering into the relationship, for example as part of the CDD process when onboarding a customer residing in or intending to do business with a HRTC. The transactions that are subsequently conducted as part of this business relationship are subject to ongoing monitoring (transaction monitoring). Approval for the continuation of the business relationship is required if the customer starts doing business with an HRTC, or in cases where transactions are made to or from an HRTC where this does not fit within the expected transaction profile of the customer.

GP3.36: Good practice - including transactions with HRTCs in the transaction profile

During onboarding, an entity asks about potential transactions involving an HRTC. When the customer indicates that it is going to conduct transactions involving an HRTC, the entity collects additional information on, among other things, the background of these transactions and considers whether they are appropriate in view of the customer's profile. The entity makes a risk analysis on the basis of this information. The customer file is submitted to senior management for approval.

GP3.37: Good practice - framework for senior management approval

An entity secures senior management approval through a 'senior management approval framework' that clearly defines:

a. The parameters within which approval is given for business relationships with customers from HRTCs. Cases that fall outside these parameters require explicit approval from senior management and need to be evaluated on a case-by-case basis. Those implementing the policy have sufficient knowledge and experience to make this assessment.
b. The frequency and method of reporting to senior management.
c. The way senior management gives approval within the framework.
d. Monitoring by the compliance and audit functions.

GP3.38: Good practice - ongoing enhanced monitoring

Before entering into a business relationship, an entity takes note of the fact that the customer will conduct transactions involving an HRTC. The business relationship is entered into after approval by senior management, according to the rules applicable within the institution.

The transactions that subsequently take place as part of this business relationship are subject to ongoing enhanced monitoring (transaction monitoring). In cases where transactions are conducted that fall outside the customer's expected transaction profile, consideration is given as to whether or not the relationship can continue.

GP3.39: 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 entity takes note of this. It analyses the transactions, using the transaction information as additional information, and determines that the customer is spending money on tourist activities. It therefore concludes that there is a low risk of money laundering and terrorist financing.

3.7 Dealing with other heightened risks and enhanced customer due diligence

Certain types of customers or products may inherently pose a heightened integrity risk. In carrying out their risk analyses, it is important that entities are alert to factors that indicate an inherently elevated risk, and that they take additional measures to mitigate integrity risk. The risk assessment must be customer-specific.

At the same time, entities should not overestimate risks, as this would lead to the excessive use of controls, with the potential consequence of bona fide customers facing a high administrative burden or being unnecessarily rejected. This underlines the importance of the risk-based approach: where risks are lower, simpler measures suffice.

Q&A

QA3.42: Question
When should an entity conduct enhanced customer due diligence?

Answer
The *Wwft* describes a number of situations where enhanced customer due diligence is required.[132]
Enhanced customer due diligence must in any case be performed in the following cases:
If a business relationship or transaction due to its nature involves a higher risk of money laundering or terrorist financing.
If the customer is domiciled, established or has its registered office in a state with a higher risk of money laundering or terrorist financing (HRTC), as designated by the European Commission under Article 9 of the Fourth Anti-Money Laundering Directive.
For complex or unusually large transactions and transactions that are part of an unusual pattern or that have no clear economic or lawful purpose.

QA3.43: Question
What factors indicate a potential high risk?

Answer
In its risk assessment, the entity must at least include the non-exhaustive list of risk factors in Annex III of the Fourth Anti-Money Laundering Directive.[133] These factors can indicate an elevated risk.

Other bodies also provide information on risk factors. For example, the EBA has published its "ML/TF Risk Factors Guidelines" and a report on the ML/TF risks associated with payment entities, and the Financial Action Task Force (FATF) has put out its own Guidance.[134]

132 Section 8(1) of the *Wwft*.
133 Section 8(2) of the *Wwft*.
134 EBA (2021), Guidelines on ML/TF Risk Factors.

QA3.44: Question
Do some sectors inherently pose high risks?

Answer
There are sectors that are generally known to be more vulnerable to integrity risks and therefore have a higher integrity risk profile. However, this does not mean that all customers in these sectors should always be assigned a high risk profile. Conversely, customers operating in low-risk sectors should not always be assigned a low risk profile.

The sector in which a customer operates is only one of the factors the entity must consider in determining the customer risk classification. This risk classification is customer-specific and therefore does not apply generically to all customers in a particular sector.

QA3.45: Question
Is cash always high risk?

Answer
No. Cash is legal tender, the legitimate use of which should not be obstructed. In principle, an entity must investigate if, for example, a transaction does not fit the profile of the customer in question, or if high-risk indicators emerge. Cash use can be an indicator, but it should always be assessed in conjunction with other indicators.

€500 notes deserve special attention. National banks in the euro area stopped issuing new €500 notes in January 2019. Although the €500 note is legal tender, transactions involving notes with relatively high denominations (€200 and €500) carry an increased risk of criminal activity.

QA3.46: Question
Does the presence of a factor indicating high risk mean that a customer must be classified as high risk?

Answer
No. Based on its risk assessment, the entity itself determines whether there is a high-risk situation that warrants enhanced customer due diligence. In doing so, it must take into account at least the risk factors listed in Annex III of the Fourth Anti-Money Laundering Directive. These factors are tools for assessing whether there is a high-risk situation. The list is not exhaustive, however, as there may also be other factors that indicate high risk.

Entities must establish policies and procedures based on their risk assessments and identify high-risk cases. The presence of a high-risk factor does not automatically imply that the customer should be classified as high risk. All relevant factors should play a role in determining the risk profile.

QA3.47: Question
Should entities reject all high-risk customers?

Answer
No. Any decision to enter into or continue a business relationship with a specific customer is up to the entity itself, and must be based in part on the institution's risk appetite and its ability to manage identified integrity risks.

QA3.48: Question
Can entities label an entire sector or group of customers with similar characteristics as unacceptable on the basis of the Wwft?

Answer
No, an the Wwft does not provide grounds to categorically label an entire sector or group of customers with similar characteristics as unacceptable.[135] An entity must evaluate customers' specific characteristics when making a risk assessment. Examples of such characteristics include business activities in sectors with an increased risk of money laundering or terrorist financing, and ties to jurisdictions that have an increased risk of money laundering or terrorist financing.

Entities must avoid unnecessarily rejecting customers or transactions by using adequate customer-specific measures based on a customer-specific risk assessment.

QA3.49: Question
What does enhanced customer due diligence entail?

Answer
In cases where there is a higher risk of money laundering or terrorist financing, the entity must implement supplementary controls (in addition to its standard controls). These measures vary depending on the institution's risk assessment with respect to the customer, transaction, product and country or jurisdiction concerned. The intensity of the customer due diligence process should be tailored to the risk level.

QA3.50: Question
Are entities allowed to identify and verify customers remotely?

Yes, they are. However, non-physical presence of the customer is considered a risk factor under Annex III of the Fourth Anti-Money Laundering Directive. Section 8 of the *Wwft* refers to this annex.

Entities must use a risk-based approach to determine what measures need to be taken to compensate for the higher risk due to non-physical presence. Measures taken under Section 8 of the *Wwft* are in addition to those that must be taken under Section 3 of the *Wwft*. The fact that customers have been accepted remotely aided by innovative technological solutions does not mean that these customers should necessarily be given a high risk rating after acceptance.

For customers who are not physically present, the entity must consult multiple independent and reliable sources or apply innovative technologies to mitigate the risk. The entity is free to design this process as it sees fit, with due attention to Sections 3, 5 and 8 of the *Wwft*. It is vital that the entity documents and regularly updates this process.

GP3.40: Good practice - collecting additional information

When accepting customers that purchase products with an enhanced risk, such as products or combinations of products which deviate from standard products, regular procedures are not sufficient. The entity must therefore do more than simply check whether the customer and other stakeholders appear on sanctions lists, whether they are creditworthy, whether their identity documents are genuine, and whether the customer appears in entities' internal or external warning systems; it must collect additional information.

135 An entity may consider on its own grounds that it focuses its services on certain sectors, and that it does not accept clients who are not active in one of those sectors.

What additional information is collected depends on the institution's customer risk profile (customer-specific). The entity considers what is required on a case-by-case basis, and additional information may include information on the customer's business activities, the reputation of the customer and of the UBOs, as well as the reputation of persons with whom they are associated. In certain cases, as part of its enhanced customer due diligence, the entity investigates the source of funds.

GP3.41: Good practice - higher risks and mitigating measures

An entity considers customers based in an HRTC or in a country with a significant level of corruption to be high risk. This also applies to customers with UBOs domiciled in high-risk countries.

If the customer is not a natural person, it is up to the entity to take measures to verify its legal status. For transactions and business relationships involving high-risk countries, the entity carries out additional checks and determines in which cases it will limit the transaction amount and frequency, and under what circumstances it will not conduct transactions at all. The entity documents this when it accepts new customers.

GP3.42: Good practice - structural and operational risks

In its policy, an entity has defined in which situations there is an increased risk in relation to legal entities. This is at least the case in relation to:

- Entities whose cash transactions exceed a percentage set by the institution, based on what is customary in the relevant industry.
- Entities with a structure consisting of more than two layers.
- Entities that have proxy shareholders or bearer shares, as these encourage anonymity.

GP3.43: Good practice - dealing with cash-intensive customers

Customers who use cash more than average are given special attention in an institution's policy. The entity sees cash as a factor that can lead to higher risk, as the origin of cash funds is more difficult to determine. The institution's policy states that additional investigations must be conducted into the origin of the financial flows of cash-intensive customers who, in conjunction with other factors, pose a high risk.

The entity has established indicators on the basis of which the depth of investigation is determined (including with regard to questioning the customer). These include the amount, the reported origin of the funds, the country of origin or destination of the funds, and the product or service provided.

At the same time, the entity avoids unnecessarily rejecting customers or transactions through customer-specific measures informed by a customer-specific risk assessment.

3.8 Risk profile

The purpose of the *Wwft* is to prevent involvement in money laundering and terrorist financing. The *Wwft* is risk-based legislation: the intensity of measures to prevent money laundering and terrorist financing should be tailored to the concrete risks posed by a customer. The higher the risk posed by the customer, the more scrutiny is called for; if the risk is lower, less intensive monitoring will be sufficient.

Identifying and analysing risks also includes classifying customers into risk categories. By establishing a risk profile entities can continuously review whether the business relationship and the transactions carried out still match the institution's knowledge of the customer and their risk profile. If, for

example, it turns out that the transactions carried out by a customer deviate from their risk profile, the entity adjusts the risk profile. On that basis, the entity can also determine whether fewer or more measures are needed to mitigate risks.

Q&A

QA3.51: Question
Should every customer be assigned a risk profile?

Answer
Yes, the risk analysis and resulting risk profile are still the starting point for risk management.

In establishing a customer risk profile, relevant risk factors identified during the customer due diligence process must be taken into account. Ultimately, the entity should have an understanding of the rationale and appropriateness of transactions and products for the customer in question, so that behaviour that may be indicative of money laundering and terrorist financing stands out.

QA3.52: Question
Can an entity make use peer groups to determine the risk profile of the customer?

Answer
Yes, it can. Entities can base the risk profile among others on peer groups. Peer groups can be defined by the entity itself on the basis of a number of customer characteristics, such as sector, legal form, age, income, country, etc.

In practice, not every customer will fit into a predefined peer group. These customers must be analysed separately.

QA3.53: Question
Does a customer's risk profile always remain the same?

Answer
No. The risk profile may change over time. By conducting a customer review, the entity can determine whether the established risk profile is still appropriate. The frequency and depth of the review should depend on the risks posed by the customer.

The customer review is part of ongoing customer monitoring.

QA3.54: Question
How does the transaction profile relate to the risk profile?

Answer
The transaction profile of the customer helps to establish the customer's risk profile. The transaction profile enables entities to sufficiently monitor transactions conducted over the course of the business relationship to ensure that these are consistent with the knowledge they have of the customer and their risk profile, and to determine if this needs adjustment.[136] A customer's expected transaction profile may be created using peer groups.

During the relationship, it is important that the entity continually monitors whether the customer fits their risk profile and whether the transaction pattern is in line with expectations. This is part of ongoing customer monitoring.

136 Section 3(2), under d, of the *Wwft*.

GP3.44: Good practice - peer groups

For lower-risk customers, an entity uses peer groups to determine a transaction profile. These customers are not questioned in advance about their expected transactions. If their actual transactions deviate from their transaction profile, the entity checks whether the profile still fits the customer and whether the customer should be reclassified. If there is a relatively high number of deviations within the peer groups, the entity checks whether these need to be adjusted.

GP3.45: Good practice - classifying customers into risk categories

An entity assigns its customers to various risk categories (low, normal, high and unacceptable) and implements control measures commensurate to the risks.

3.9 Recording data

Entities must keep retrievable records of documents and data relating to customer due diligence.[137] This enables entities to substantiate their customer risk profiles and to identify and assess behavioural/transaction patterns in a timely manner. Internal and external supervisors can also assess the institution's compliance with the *Wwft* based on these records. Finally, the entity can provide data to FIU-NL and investigative agencies where necessary.

Q&A

QA3.55: Question
What documents and data need to be recorded?

Answer
Section 33 of the *Wwft* specifies what documents and data entities must at least record. It is important that the customer file includes a risk profile and its substantiation.

The data that has to be recorded is the data obtained during the CDD process, such as copies of identity documents, account information, correspondence, notes on conversations about and with the customer, transactions effected by the customer and information about other services provided to the customer. Section 33(2) Wwft determines which documents and data have to *at least* be recorded. The customer file should also show how the customer acceptance decision-making process went.

The "Personal Data Identification and Verification" Guidelines of the Dutch Data Protection Authority state that a financial institution can also record a copy of a verified identity document as proof that the identification requirement has been met (reconstruction obligation).[138] Pursuant to Section 33 of the *Wwft*, there is no obligation to record the customer's citizen service number (BSN). The Dutch Data Protection Authority's website also offers information on the kind of data banks can and cannot retain.[139]

137 Section 33 of the *Wwft*.
138 wetten.overheid.nl/BWBR0033181/2012-07-12.
139 autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/financiele-ondernemingen.

QA3.56: Question
How long should documents and data be retained?

Answer
Entities must keep documents and data for five years after terminating the business relationship or conducting the transaction in question.[140]

QA3.57: Question
Does it matter how documents and data are recorded?

Answer
Yes, it does. The entity must record documents and data in a retrievable manner.[141] Documents and data must also be accessible.[142]

The entity must have systems in place that enable it to respond promptly and adequately to inquiries from FIU-NL and the supervisory authority.[143]

GP3.46: Good practice - recording documents and data in customer file

An entity records all documents and data related to customer screening in its customer files. These customer files are easily accessible, including to analysts within the entity who assess signals from transaction monitoring, and to the compliance officer.

GP3.47: Good practice - customer acceptance committee

An entity has set up a customer acceptance committee in which senior executives discuss and decide on complex cases. These discussions and decisions are consistently documented in an accessible location. The follow-up of decisions and any additional mitigation measures are monitored and documented by a designated officer.

3.10 Within risk tolerance?

A customer may fall outside an institution's risk tolerance with regard to money laundering or terrorist financing. This means that the entity has concluded, based on the customer due diligence process and the established risk profile, that an existing or proposed business relationship with a customer poses excessive integrity risks.

In some cases, the *Wwft* prescribes that a customer may not be accepted, or that an existing business relationship must be terminated.[144]

140 Section 33(3) of the *Wwft*.
141 Section 33(1) of the *Wwft*.
142 Section 33(3) of the *Wwft*.
143 Section 33(4) of the *Wwft*.
144 See Sections 4 and 5 of the *Wwft*.

Q&A

QA3.58: Question
What are the considerations in determining whether the customer is within the risk appetite?

Answer
An entity defines in its policy which risks are acceptable, and which risks are not acceptable, taking into account legal requirements regarding, for example, HRTCs. The entity then assesses on an individual basis whether or not a customer is within the risk tolerance. This is related to the risk profile.

An entity can determine in advance that certain risk profiles – which could for example be attributed to peer groups – can be accepted, possibly under certain conditions.

QA3.59: Question
Should an entity eliminate any risk of involvement in money laundering or terrorist financing?

Answer
No. As part of their role as gatekeepers, entities guard against criminal money flows from entering the financial system. In accordance with the spirit of the *Wwft*, their actions in this context must be based on a risk assessment. After all, the entity itself cannot fully exclude that a customer is involved in money laundering or terrorist financing.

The decision to enter into a business relationship must be based on an informed risk assessment and on the institution's ability to manage these risks.

Entities are thus expected to have all reasonable measures in place to prevent them from facilitating criminal financial flows. The use of a risk-based approach also means accepting that, despite mitigating measures, criminal money will flow through the financial system. Entities are not expected to completely eliminate this, so there is an accepted "residual risk".

QA3.60: Question
Does DNB decide which customers can or cannot be taken on?

Answer
No, the entity decides which customers it does and does not accept. The entity makes this decision based on its obligations under the Wwft, its control measures and its risk tolerance.

GP3.48: Good practice - risk tolerance policy

In its policy, an entity has set out in which cases (based on its legal obligations) customers should not be accepted and existing relationships should be terminated, and in which cases customers fall outside the institution's own risk tolerance, for instance if:

- there are problems in verifying the identity of the customer or the UBO;
- a customer wishes to remain anonymous or provides fictitious identity details;
- shell banks are involved (banks incorporated and licensed in a jurisdiction where they have no physical presence);
- a customer is on a sanctions list;
- additional information reveals that the combination of customer type and desired products poses unacceptable risks;
- a customer is unwilling to provide full information (or is unable to provide adequate documentation to verify such information) concerning their nature and background, the purpose of the business relationship and in particular the source of their assets;
- a customer's organisational structure and/or the purpose of the structure of which the object company is a part is (are) found upon examination to be unnecessarily complex or non-transparent, without there being a logical commercial explanation for this;
- professional counterparties lack the required licences;
- a customer does not give the service provider sufficient insight into their structures, cash flows and/or tax motives.

GP3.49: 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 in which economic activity takes place. The UBO of the bakery is citizen of a known European tax haven and controls the structure from a South American jurisdiction. The bank judges that the customer structure is outside its risk tolerance.

3.11 Accept and attribute level of control

If a customer falls within an institution's risk tolerance, they can be accepted. As part of its risk management, the entity subsequently uses mitigating measures to monitor the business relationship. The intensity of these controls should match the customer's risk profile so that they are tailored to the concrete risks of money laundering and terrorist financing posed by the customer. The higher the risk posed by the customer, the more scrutiny is called for; if the risk is lower, less intensive monitoring will be sufficient. This in turn is important for proper access to the financial infrastructure, and to ensure that the administrative burden on both the customer and the entity is proportionate.

Q&A

QA3.61: Question

To what extent can an entity accept a customer before customer due diligence has been completed?

Answer

Customer due diligence must take place before the entity enters into a business relationship or performs a non-recurring transaction.[145]

There are, however, some exceptions:

- An entity is permitted to verify the identity of the customer and the UBO during the process of entering into the business relationship, provided that this is necessary for the continuity of service provision and there is limited risk of money laundering or terrorist financing. In that case, the entity must verify the identity as soon as possible after the initial contact with the customer.[146]
- Verification of the identity of the beneficiary of a life insurance policy takes place at the time of payment of the life insurance policy.[147]
- A bank or other financial institution may 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.[148] This also applies to payment institutions. The payment institution may not transfer funds to a merchant before identity verification has taken place, it may however begin collecting.[149]

145 Sections 4(1) and 5(1) of the *Wwft*.
146 Section 4(3) of the *Wwft*.
147Section 3a(2) of the *Wwft*.
148 Section 4(4) of the *Wwft*.
149 See Section 4(3) of the *Wwft*.

GP3.50: Good practice - additional measures

An entity applies the following additional measures for higher-risk customers:

- More frequent reviews of the business relationships.
- Deeper investigation into the rationale behind transactions, and into the origin of funds.
- Mandatory advice from the compliance department on accepting or continuing the business relationship.
- "Bad press" monitoring.

3.12 Refusing customers

It is important that criminal money flows are kept out of the financial system. Entities should therefore avoid accepting customers who pose an unacceptable risk.

Q&A

QA3.62: Question

When should an entity not accept a customer?

Answer

An entity should not accept a customer if:

- no customer due diligence has been carried out (subject to the exceptions listed in QA3.61);[150]
- customer due diligence has not yet been completed;[151]
- customer due diligence has not led to the intended result;[152]
- the entity does not have all the required identification and verification data, or other relevant data on the identity of the customer, UBO and any representatives;[153]
- a customer poses an unacceptable risk to the institution.

GP3.51: Good practice - customer acceptance policy

In its customer acceptance policy and work instructions, an entity has clearly set out under which circumstances customer relationships must be refused.

3.13 Reporting to the Financial Intelligence Unit (FIU-NL)

If customer due diligence does not lead to the intended result or a business relationship is terminated, and if the entity has indications that the prospective customer is involved in money laundering or terrorist financing, the entity must report this to the Financial Intelligence Unit (FIU-NL).[154]

In addition to the above cases, entities must report unusual transactions (proposed or completed) without delay after the unusual nature of the transaction becomes known – see also Section 4.1.5.

150 Section 5(1), under a, of the *Wwft*.
151 Subject to some exceptions, such as those listed in Section 4 of the *Wwft*.
152 Section 5(1), under b, of the *Wwft*.
153 Section 5(1), under c, of the *Wwft*.
154 Section 16(4) of the *Wwft*.

GP3.52: Good practice – Substantiated report

An entity receives a request from a company for financing. A business loan to finance leased out real estate. Further investigation brings light to various remarkable points. The company show a rapid growth in its real estate portfolio in a short amount of time. Furthermore there are cases wherein the residences were sold by private persons to the company below the assessed value, while the private persons would have been able to get a higher price on the market.

The entity decides to report this intended transaction to FIU-NL. The unusual transaction report sets out which product the customer requested and which considerations have lead to the conclusion that the intended transaction was unusual. The circumstances are recounted in detail in the transaction description and all parties involved are named in the unusual transaction report.

GP3.53: Good practice – Substantiated report

A bank reports several unusual transactions relating to the sale and purchase of vehicles. The report shows that the entity has performed an extensive investigation into open sources. The bank provides this information, which amongst others shows that the parties which appear to be car dealerships, do not have any online presence and are registered to a home address. Also, a number of counterparties raise suspicion because there is a relation to a large fraud case referred to in the unuusal transaction report. The provided information also makes clear that cars are being bought by parties active in other sectors, and that the company recieves rental payments for trucks, whereas this not part of the business model of the company.

The description provided by the entity does not only recount all the transactions, but also provides details on why the transactions are unusual. Multiple transactions are reported, which are connected in the report.

As an annex the entity includes a complete overview of the bank account throughout the relevant time period, which provides context and insight into the transactions of the customer. This allows the FIU analyst to start in investigation without delay.

4 Customer due diligence: ongoing monitoring

4.1 Transaction monitoring

Entities are required to monitor on an ongoing basis their business relationships and the transactions conducted over the course of those relationships.[155] They must do so for the following reasons:

- To ensure that the transactions match the institution's knowledge of the customer and their risk profile.[156]
- To keep out criminal financial flows.
- To (be able to) detect and report unusual transactions.[157]
- To ensure that customer data is kept up to date.[158]

Financial crime undermines the foundations of our society. As gatekeepers of the financial system, financial institutions play an important role in preventing this. An entity that adequately monitors the transactions carried out as part of its services 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.

- The entity can investigate such transactions and, if necessary, report them to FIU-NL. FIU-NL can then analyse the transactions and, if there is reason to do so, pass them on to the investigative authorities.
- It can also detect and reject transactions if it suspects that they are related to money laundering or terrorist financing.

Inadequate monitoring makes entities vulnerable, and can cause them to (unwittingly) contribute to terrorist financing or money laundering.

Transaction monitoring is thus an essential measure to detect potential criminal money flows. Entities must pay particular attention to unusual transaction patterns and transactions that, due to the nature of the customer, typically carry a higher risk of money laundering or terrorist financing.[159] If there are grounds to assume that a (proposed) transaction is linked to money laundering or terrorist financing, entities must immediately report this to FIU-NL.[160]

Q&A

QA4.1: Question
What is a transaction?

Answer
The term "transaction" is understood to mean: "an act or a combination of acts performed by or on behalf of a customer of which the entity has taken note in the provision of its services to that customer."[161] This definition includes more than just payment transactions, for example.

155 Section 3(2), under d, of the *Wwft*.
156 Section 3(2), under d, of the *Wwft*.
157 Section 16(1) of the *Wwft*.
158 Section 3(11) of the *Wwft*. Section 14(4) of the *Bpr*.
159 Section 2a(1) of the *Wwft*.
160 Section 16(1) of the *Wwft*.
161 Section 1(1) of the *Wwft*.

The definition of transaction is intended to make clear that an unusual transaction by the customer or by a third party acting on behalf of the customer must always be reported if the entity has become aware of it in the course of providing services to that customer. It is not a requirement that there must be a direct or causal connection between the unusual transaction and the activities of the institution. 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 entity (by virtue of its knowledge of the transaction) can also trigger the statutory reporting obligation.[162]

QA4.2: Question
What is an unusual transaction?

Answer
An unusual transaction within the meaning of the *Wwft* is a transaction which, based on the indicators referred to in Section 15(1) of the *Wwft*, qualifies as unusual. These indicators are listed in the annex to Section 4 of the Decree implementing the Anti-Money Laundering and Anti-Terrorist Financing Act 2018 (*Uitvoeringsbesluit Wwft 2018*).

The indicators are divided into objective and subjective indicators.

- The objective indicators describe situations in which transactions must always be reported without delay.
- Subjective indicators force an entity to report a transaction if it has reason to suspect that a transaction may be related to money laundering or terrorist financing. This requires the entity to assess whether a transaction is unusual.

Where indicators are related to a specific transaction limit, the entity should also assess whether there is a connection between two or more transactions. This can be done on the basis of the type of transaction and the amounts involved. If there is a connection and the transactions together exceed the limit, the entity reports them as a subjective indicator – even if it is not entirely certain that the transactions are linked, but there are well-founded suspicions.

QA4.3: Question
Should transaction monitoring always be automated?

Answer
No. Entities must set up the transaction monitoring process in a risk-based manner. The design should depend, among other things, on the nature and size of the institution, the risks it faces and the number of transactions it carries out.

The use of automated transaction monitoring is not required. However, if there are large numbers of transactions, it is appropriate to have an automated transaction monitoring system in place to be able to safeguard the effectiveness, consistency and processing time of the monitoring. The point is that entities must effectively detect unusual transactions and potential criminal money flows.

QA4.4: Question
Designing transaction monitoring is a dynamic process; what does that mean?

Answer
Chapter 2 states that a risk analysis should be the starting point for the design of controls, including transaction monitoring. The risk analysis identifies the relevant and most important risks related to

162 *Parliamentary Papers II*, 2011–2012, 33 238, no. 3, p. 10. Legislative history offers several relevant examples. For instance, an auditor may notice an unusual transaction in a customer's records. Or a notary might learn of an unusual price difference between the AB and BC transactions for the purpose of an ABC delivery. Similarly, a bank may notice an unusual value in a trading transaction.

money laundering and terrorist financing. On the basis of this assessment, the entity then determines how transaction monitoring should be set up to verifiably manage risks.

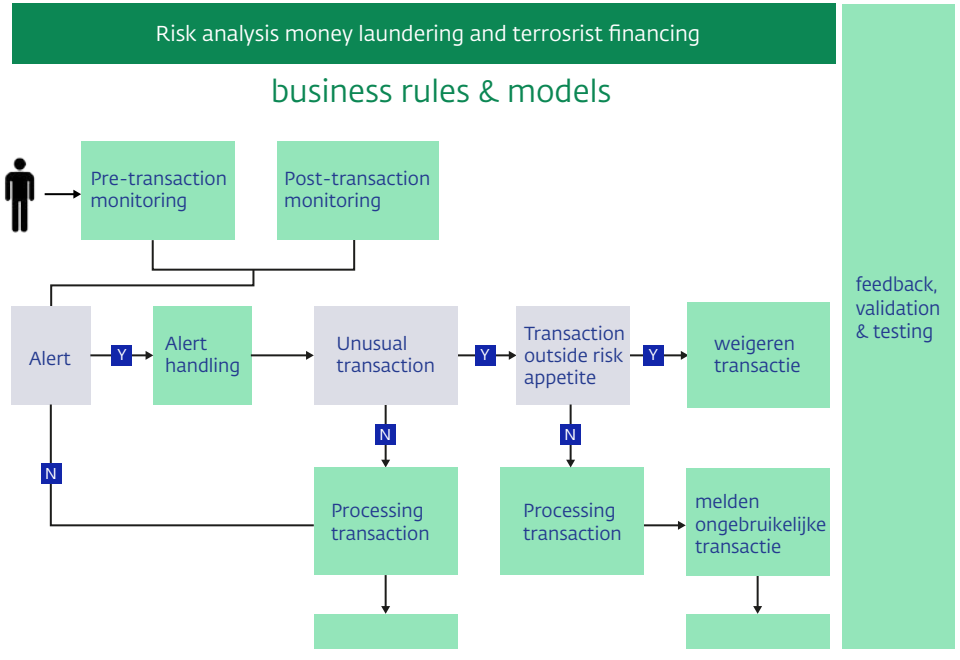
Because risks change, this is a dynamic process:

- Based on the nature and extent of the risk (e.g. cash, payments to high-risk countries), the entity determines which business rules and models (with associated thresholds) can detect the risk.
- Using historical transaction datasets, the entity tests whether the risks are adequately detected with the chosen business rules, models and limits, after which it proceeds to implement them in its operations.
- Subsequently, the entity monitors whether the output of the transaction monitoring system is consistent with the identified risks and documents its considerations.
- If the entity determines that a risk is not yet adequately detected, it may introduce additional mitigation measures.

It can be used as an aid when reading this chapter, and as a way of mapping out the various components of the transaction monitoring. The element at the top of the chart, the money laundering and terrorist financing risk analysis, has already been discussed in Section 2.1. The risk analysis is the starting point for drafting policies and procedures related to transaction monitoring. This leads to the business rules and models. These business rules and models provide a basis for transaction monitoring. Using validations and feedback-loops the entity improves the business rules and models where necessary.

In the sections below, the following elements are discussed:

- business rules & models;
- pre-transaction monitoring;
- post-transaction monitoring;
- alert handling;
- reporting unusual transactions;
- feedback and testing.



Elements of transaction monitoring

A number of elements related to transaction monitoring are explained here. This explanation is based on the chart below, which outlines the transaction monitoring process. This chart is intended to structure transaction monitoring discussions; it does not show a course of action prescribed by the *Wwft*.

4.1.1 Business rules & models

An entity's risk analysis should inform the measures it takes to combat money laundering and terrorist financing. The same is true for transaction monitoring. The knowledge that the entity applies to detect unusual or suspicious transactions is tailored to the risks it faces.[163] E.g., the business rules implemented by an entity should be appropriate for the detection (and mitigation) of the risks named in the risk analysis and the scenarios used in that analysis.

Recognising or detecting unusual or suspicious transactions thus requires more than general knowledge of typologies, for example. What is needed is insight into how the entity could become involved in money laundering or terrorist financing, given its business and operations.

Q&A

QA4.5: Question
Is it enough if an entity applies standard models for detecting unusual transactions?

Answer
No. Standard models can be a starting point, but entities need to do more. A transaction monitoring system should fit the institution's risk profile, and be fed by the institution's own applied knowledge (intelligence). The transaction monitoring system's business rules should enable the effective mitigation of the risks faced by the institution. The entity must document how its risk analysis informs its transaction monitoring system.

QA4.6: Question
Is it mandatory to create a transaction profile based on expected transactions?

Answer
The entity must establish the customer's risk profile.[164] Together with this risk profile, a transaction profile based on the expected transactions or use of a customer's account (expected transaction profile (ETP)) can be a useful tool for detecting unusual transactions. By identifying the expected transaction behaviour, entities can assess whether the transactions carried out are consistent with what they know about the customer.

In this context, however, the ETP should be seen as a means and not an end in itself. Unusual transactions can also be detected using other methods, for instance by applying scenarios or advanced modelling.

QA4.7: Question
To what extent can peer groups be used?

Answer
It is not always possible to draw up individual tailored risk profiles for each individual customer in advance, especially given the large number of customers in specific segments, such as banking services for private individuals or SMEs. Instead, entities can opt for a more practical approach by categorising their business relationships according to peer groups, for example, and base the individual risk profile on that. Peer 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. An ETP can also be created for a peer group. This does require the peer groups to be sufficiently homogeneous in terms of customer behaviour.

163 Compare to Sections 2a-2c of the *Wwft*. An entity is extra vigilant regarding unusual transactions patterns and transactions that by their nature constitute a higher risk of money laundering or terrorist financing.
164 Section 3(2), under d, of the *Wwft*.

QA4.8: Question
Is there a model that is applicable to all entities? No. An institution's business rules and models should be tailored to the risks it is exposed to. This means that the entity itself must determine which business rules and models are relevant to its operations. That is why it is important to base the design of the transaction monitoring system on the outcomes and insights from the risk analysis. In doing so, the entity provides insight into what the most significant risks in its customer portfolio are, and into how its transaction monitoring system contributes to detecting and mitigating these risks.

As entities evolve and risks change, the entity must establish a process to systematically monitor and assess (and adjust, where necessary) the effectiveness of the business rules and models used.
The entity must always be able to detect unusual transaction patterns and transactions which by their nature carry a higher risk of money laundering or terrorist financing.[165]

GP4.1 Good practice - intelligence and transaction monitoring

Intelligence (applied knowledge about customers and typologies) can contribute to effective transaction monitoring:

- Entities that process a limited number of transactions may be able to suffice with manual transaction monitoring. In these cases, too, applied knowledge (laid down in a manual or work instructions, for example) must be used to detect unusual or suspicious transactions.
- Entities that use automated transaction monitoring generally use instructions and detection rules to detect potential money laundering and terrorist financing patterns, for example in the form of scenarios and associated transaction limits (business rules).
- Entities may also use models, artificial intelligence (AI) or machine learning for this purpose. They might, for instance, use models that can detect customers exhibiting outlier behaviour (relative to their peer group). Models that perform network analyses can also be used, or models that are able to analyse transaction data using historical FIU-NL reports to identify transactions with similar characteristics.

GP4.2 Good practice - link with risk analysis

An insurer has created a set of business rules for the purpose of its transaction monitoring. In these business rules, the insurer has incorporated the risks and scenarios identified in its SIRA. One of the SIRA scenarios that has been translated into a business rule concerns the detection of transactions related to early surrender above a certain limit. For these transactions, the entity performs a plausibility check by default (if this has not already been adequately performed at an earlier stage). This plausibility check includes the entity checking whether the premiums deposited are explicable.

GP4.3 Good practice - creating business rules

An entity is able to substantiate the choices it made in designing its business rules, and it can demonstrate the adequacy of these rules. The entity has paid attention to:

- clearly defining its limit values;
- differentiation in the business rules between limits for high-risk customers in the context of enhanced monitoring;
- differentiation in the business rules between limits for various business segments (SMEs, corporate, financial institutions).

165 Section 2a(1) of the *Wwft*.

GP4.4 Good practice - linking business rules and risk analysis

A bank creates the business rules for its transaction monitoring system based on its risk assessment (SIRA), The bank also documents the connection between its SIRA and the business rules.

In preparing its business rules, the bank takes various factors into consideration, such as:

- the type of customer (private individual or business customer);
- the customer segment, for instance by making a distinction between private banking and retail, and breaking these categories down into other segmented target groups, such as professional athletes;
- the customer risk profile that was created during CDD and possibly adjusted at a later stage;
- the transaction's country of origin or country of destination;
- the product (e.g. savings, real estate finance or trade finance);
- the distribution channels (e.g. physical presence of the customer or online);
- the nature and frequency of transactions (e.g. cash or non-cash);
- the customer's risk profile classification (e.g. low, medium or high);
- international transactions effected from off-shore countries through the Netherlands to other off-shore countries.

Furthermore, the bank also uses comparisons with the customer's other transactions and with the customer's peer group in determining the business rules. The business rules not only take into account the factors mentioned above; they also substantiate the thresholds the entity sets, based on data where possible. The risks detected by the entity should be included in the evaluation of the SIRA.

GP4.5 Good practice - business rules for terrorist financing

To detect terrorist financing, an entity has a list of red flags and possible business rules that may indicate terrorist financing. To keep this list up to date, the entity uses warning lists and published cases and typologies.

GP4.6 Good practice - spotting unusual transactions using outlier detection

An entity uses data analysis and modelling to detect outliers. In doing so, it looks at transaction volumes, numbers of transactions, transactions to high-risk countries or sectors, and anomalous patterns in IP address data or other technical characteristics. As a result, the entity also detects unusual transactions that it would not be able to identify using only its business rules. The entity uses the outcomes of this analysis to adjust its risk appetite.

GP4.7 Good practice - risk appetite and business rules

For the purposes of its risk analysis, an entity has defined its risk appetite. It has also identified which activities (in terms of their nature and size) fall outside its risk appetite. The entity then uses its risk appetite by translating it into business rules, defining appropriate limits 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 limits are flagged by the transaction monitoring system, after which they are investigated.

GP4.8 Good practice - cash

A bank has included rules regarding the use of cash in its set of business rules. These rules are based on the bank's risk analysis. The bank has also defined its risk appetite. This states that for small and medium entities, cash transactions below a certain threshold should not generate an alert. In determining this threshold, the nature of the business is taken into account.

The bank's business rules for cash allow it to detect excessive cash usage and the frequent use of large denominations that do not fit the customer's business model. No alerts are generated for customers making individual transactions below the threshold set by the bank, in absence of further particularities.

GP4.9 Good practice - high-risk jurisdictions

An institution's transaction monitoring system pays extra attention to high-risk jurisdictions. To identify high-risk jurisdictions, the entity 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.
- Pre-transaction monitoring and suspected ML/TF transactions

Entities may in any case not conduct transactions that facilitate money laundering or terrorist financing, or where there is a suspicion that this is the case. For other transactions entities should also consider whether they, based on the risks of ML/TF, can be executed. It is important that entities take adequate measures to detect unusual transactions even before they are carried out.

Pre-transaction monitoring occurs before a transaction is completed. Through pre-transaction monitoring, unusual transactions, or other transactions that fall outside of the risk tolerance of the entity, can potentially be detected even before they are executed, or while they are being executed. Suspected ML/TF transactions should always fall outside the institution's risk tolerance, and must therefore me rejected.

Q&A

QA4.9:Question

What kind of transactions should be considered suspicious?

Answer

A suspected ML/TF transaction means that there is a significant likelihood that the transaction will facilitate money laundering or terrorist financing, which must be determined on a case-by-case basis.

Besides suspected ML/TF transactions, there may also be other unusual transactions that fall outside the institution's risk tolerance. This could for example be the case when the entity has reason to suspect there is ML/TF and further investigation into the transaction and source of funds do not alleviate the doubts.

Entities must pay extra attention to complex or unusually large transactions, to transactions that are part of an unusual pattern and to transactions without a clear economic or legitimate purpose. These transactions must be investigated.[166]

166 Section 8(3) of the *Wwft*.

QA4.10:Question
How should pre-transaction monitoring be set up?

Answer
Pre-transaction monitoring can be either automated or manual. The process must allow the entity to detect unusual transactions even before they are executed and stop them where necessary.

GP4.10: Good practice - business rules
An entity has established specific guidelines that allow employees to determine whether a proposed transaction is unusual. Transactions that meet the criteria are referred to the compliance officer and, after a final assessment to determine whether they are in fact unusual, may be reported or refused.

GP4.11: Good practice - growing transaction amounts, refusing services
A money transfer agency notices that one of its customers regularly transfers money to the Philippines for "family support". In two months, the total amount transferred is over €10,000. After a brief investigation, the agency concludes that there is no plausible explanation for these transactions. The transactions that have already been carried out are reported to FIU-NL.

The next day, the customer wants to deposit €3,000. Upon inquiry, the customer is unable to provide a plausible explanation for the transaction amounts, nor is the customer able to explain how he acquired the money. The entity strongly suspects that the customer is involved in money laundering and refuses the transaction. The entity also files a police report and reports the proposed transaction to FIU-NL.

GP4.12: Good practice - insurer refuses policy surrender
A customer takes out a policy with an insurer. Through an intermediary, the customer deposits €750,000. Four months later, the customer wants to terminate the policy, demanding a surrender charge from the insurer.

The insurer concludes that there is a substantial likelihood that this would facilitate money laundering, and refuses the surrender. The deposit and intended surrender are reported to FIU-NL. The insurer also files a police report.

GP4.13: Good practice - suspected money laundering transaction
A bank is involved in the sale of a property owned by customer who has filed for bankruptcy. Proceeds from the sale will accrue to the bank. 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 wealth 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, notifies the police and files a report with FIU-NL.

GP4.14: Good practice - products do not match customer profile

When a customer applies for documentary credit with a bank, it notices that the products involved are different from the customer's regular business. The transaction is put on hold and reported to the compliance officer. The compliance officer 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. Evidence of this is provided. The compliance officer approves the transaction, after which it is effected. The account manager updates the customer file.

4.1.3 Post-transaction monitoring & detection of unusual transactions

Post-event transaction monitoring allows entities to identify transactions and transaction patterns that indicate possible involvement in money laundering or terrorist financing. Applied knowledge, for example in the form of business rules and models, is crucial for generating the right alerts.

Q&A

QA4.11: Question
Must post-event transaction monitoring be automated?

Answer
No. The design of the post-event monitoring process is strongly dependent on the nature and size of the entity and the number of transactions it conducts on a daily basis.

Based on the risks involved, an entity may opt for either manual or automated monitoring, or for a combination of the two. If there are large numbers of transactions, it is appropriate to have an automated transaction monitoring system in place to be able to safeguard the effectiveness, consistency and processing time of the monitoring.

QA4.12: Question
What is an alert?

Answer
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. Alerts should be generated by an institution's transaction monitoring system, but they can also come from other sources. The entity must follow up on alerts (see the section on alert handling (4.1.4) below).

QA4.13: Question
What kind of transactions should entities monitor?

Answer
Under the *Wwft*, an entity must monitor transactions related to the services it provides. A payment from the entity itself to one of its own suppliers, for example, falls outside the scope.

The entity must ensure that all source systems used for transactions that must be monitored are identified and that all the relevant data is included in the transaction monitoring process. This can be data concerning the customer, the services or the transactions.

GP4.15: Good practice - various alert generation methods

An entity uses a combination of detection methods.

- Part of the monitoring is done using business rules, allowing the entity 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 entity to check whether typologies that are relevant given its risk profile occur in its transactions.
- Another part of the monitoring is done using AI and models. This allows the entity to better detect and investigate potential unusual patterns and complex transactions.

GP4.16: Good practice - alert generation for combined transactions

An entity notices that a customer is depositing a number of relatively small amounts in a short period of time. The individual amounts, which all have the same destination, fall below the objective indicator limit, but exceed it when added up.

The transaction monitoring system generates an alert. The entity investigates the alert and concludes that the customer is probably deliberately staying below the reporting threshold. The entity labels the transactions as unusual (based on a subjective indicator) and reports them to FIU-NL.

GP4.17: Good practice - alert generation for terrorist financing

An entity 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 entity 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.

GP4.18: Good practice - transaction patterns

An entity uses its transaction monitoring system 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 use of predictive analytics allows the entity to detect broader transaction patterns, structures and networks of transactions in an automated and standardised way.

GP4.19: Good practice - ensuring data quality and completeness

An entity ensures the quality and completeness of the data it uses in its transaction monitoring system by applying technical separation of functions (e.g. between test, acceptance and production environments) and by checking the data for completeness.

The entity has predetermined which transactions and associated data must be monitored, using data trace analysis to ensure that systems and data are identified down to the attribute level. On the basis of this information, the entity has established controls for the source systems and for the transaction monitoring system. These controls ensure both the quality of the data and its completeness.

4.1.4 Alert handling

An alert is a signal indicating a potentially unusual transaction. Entities must investigate alerts (and combinations of alerts) to assess whether the transaction in question is in fact unusual.

Alert handling and assessment are important:

- Every alert must be handled. An entity cannot run the risk that unusual transactions go undetected, and that these transactions are not reported to the FIU-NL.
- Alerts cannot be reported as unusual transactions without investigation, as this could lead to erroneous reports or unjustified rejections of transactions.
- The assessment of an alert may lead to a reassessment of the customer's risk profile.

Q&A

QA4.14: Question

When should an alert be reported?

Answer

An alert is a signal. If there is an alert (or a combination of alerts), the entity must investigate whether an unusual transaction has taken place using customer and transaction data. Where necessary, external sources should be consulted, and the customer can be asked about the background and purpose of the transaction.

The investigation of the alerts and the findings must be documented. If the entity concludes that an unusual transaction has taken place, it reports this to FIU-NL.

QA4.15: Question

What requirements must alert handling meet?

Answer

Entities must have procedures and working processes in place to assess and handle alerts. Relevant staff should have up-to-date instructions and training to recognise unusual transactions and suspected ML/TF transactions.[167]

These procedures and working processes should ensure that the processing time from generating an alert to a report being filed with FIU-NL is as short as possible, and that the right priorities are set when dealing with alerts.

Moreover, it is important that entities document their considerations and conclusions with regard to closing an alert or reporting the transaction as unusual to FIU-NL.

QA4.16: Question

When is a transaction unusual?

Answer

If a transaction matches certain indicators, it qualifies as unusual.[168] Indicators have been established for different categories of entities.[169]

- The objective indicators describe situations in which transactions must always be reported.
- The subjective indicators pertain to situations where an entity has reason to assume that a transaction may be related to money laundering or terrorist financing.

167 Section 35 of the Wwft.
168 Section 15(1) of the *Wwft*.
169 Section 4 in conjunction with Annex 1 to the *Wwft implementation decree*.

The presence of subjective indicators must be assessed by the entity itself, in line with the risk-based approach.

Where indicators are related to a specific limit, the entity should also assess whether there is a connection between two or more transactions. This can be done on the basis of the type of transaction and the amounts involved. If a connection is shown to exist, these transactions could be reported as unusual based on a subjective indicator.

QA4.17: Question
If an employee concludes that a transaction is unusual, what kind of follow-up should there be?

Answer
The organisation should be structured such that the first line has a clear responsibility for transaction monitoring, and that the compliance function (if the entity has one) oversees the process and advises. The compliance function should also have a role in reporting unusual transactions to FIU-NL.[170] It is therefore important that the entity has a procedure in place that ensures the compliance function's involvement if an unusual transaction is detected.

QA4.18: Question
When can alerts be closed automatically?

Answer
An entity can automatically close certain alerts based on the risks involved. The following points should be considered here:

- The entity should have explicitly defined its risk appetite with regard to certain transactions.
- The entity should have thoroughly documented its underlying risk-based decision model.
- A relatively large number of automated closed alerts may indicate an inadequate decision model.
- The entity should have a procedure in place to ensure that alerts that are closed automatically are evaluated, for instance to detect unusual transaction patterns.

GP4.20: Good practice - documentation

As part of its alert handling, an entity documents whether the transaction fits the customer's transaction behaviour, and whether the transaction is logical and plausible for the type of customer and the sector in which the customer is active.

GP4.21: Good practice - training programme

An entity has an annual training programme for its first, second and third line. 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 entity dealt with them.

The training sessions thus translate practical experience and legislation into policies, procedures and underlying work processes. Employees are also trained on how to use the various new and existing sources available for analysis. Through these training programmes, the entity offers employees clear guidelines on how to act when faced with suspicious transactions.

170 Section 2d(3) of the *Wwft*.

GP4.22: Good practice - analysis capacity and resources

An entity gives its analysts enough time to thoroughly investigate and document their research. They also have access to adequate resources, and to internal and external systems and information sources.

This means that they are able to consult the customer file when assessing alerts. The customer file can provide additional information for detecting transactions with an elevated risk of money laundering and terrorist financing. An analyst can, for example, use the information from the customer file to assess whether the transactions are in line with the customer's activities. Another information source offers insight into the denominations used for withdrawals and deposits.

The entity uses management information on trends in the number of alerts opened and handled to ensure sufficient capacity and resources.

GP4.23: Good practice - alert analysis

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

The transaction analysis shows that frequent cash deposits are made into this 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. Even in the summer period, the ratio between cash and non-cash income has remained below the institution's threshold. 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.

It is also established that the outgoing transactions mainly involved wage payments, wholesaler purchases, taxes and rent. This is in line with the regular business activities of a hospitality establishment.

Based on the analysis, the alert handler concludes that the cash deposits are not unusual. No report is filed.

GP4.24: Good practice - terrorist financing alert analysis

Two months after a debit card transaction in eastern Turkey, a customer applies for a €10,000 loan from their bank. A bank employee finds that this customer has 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.

The employee decides to expand the investigation and finds that the funds from the first loan were almost immediately transferred to Turkey across several transactions. The employee also suspects a connection with the previous alert, for the debit card transaction in Turkey.

On the basis of this information, the employee asks the customer several questions, but they are unable to provide a clear explanation for the transactions. The bank decides to refuse the second loan and labels all transactions – the debit card transaction and the two loan applications – as unusual. The following elements/red flags play a role in this decision:

- a debit card transaction in the Turkish-Syrian border area;
- taking out a loan and withdrawing the full amount shortly afterwards;
- the use of the loan does not correspond with the customer's statement;
- funds are divided into smaller amounts for transfer;
- funds obtained as loans were transferred to certain countries.

4.1.5 Reporting unusual transactions

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

Q&A

QA4.19: Question
When should an entity report a transaction?

Answer
An entity must report executed or proposed unusual transactions to FIU-NL without delay upon their unusual nature becoming known.[171]

QA4.20: Question
When should a transaction that has been reported to the police or the Public Prosecution Service (OM) in connection with money laundering or terrorist financing also be reported to FIU-NL as an unusual transaction?

Answer
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 should also be reported to FIU-NL, given the assumption that these transactions may be related to money laundering or terrorist financing.[172]

QA4.21: Question
Are there legal consequences for the entity if a report is filed with FIU-NL?

Answer
The importance of the reporting duty is underlined by the criminal indemnification laid down in Section 19 of the *Wwft* and the civil indemnification laid down in Section 20 of the *Wwft*:

- Criminal indemnification ensures that data or information provided by an entity that reports an unusual transaction in good faith cannot be used in a criminal investigation or prosecution of that entity on suspicion of money laundering or terrorist financing. The law extends this indemnification to the person who files the report and employees who helped write the report. When an entity reports information to the FIU in accordance with the requirements of the Wwft, the entity cannot be prosecuted for sharing this information with the FIU.
- Civil indemnification means that an entity cannot be held liable under civil law for the loss suffered by another party (e.g. the customer or a third party) as a result of a report as long as the entity

171 Section 16(1) of the *Wwft*. Section 16(4) of the *Wwft* also *specifies situations that must* be reported (see Section 3.13).
172 Annex 1 to the Wwft implementation decree.

acted on the reasonable assumption that it was fulfilling its reporting duty. For instance, claims in civil proceedings could be brought for breach of contract if the entity decided not to carry out a transaction but to report it. Legal action in response to an unlawful act is also possible, if a customer claims alleged loss suffered as a result of an institution's unusual transaction report.

These indemnifications apply if the report was filed correctly and in good faith, in accordance with the requirements of the *Wwft*.

QA4.22: Question
What data must be reported to FIU-NL?

Answer
The *Wwft* stipulates what information must be provided to FIU-NL when a report is filed.[173]
FIU-NL can use this data to further analyse an unusual transaction. If an entity systematically fails to provide certain data, FIU-NL can notify the supervisory authority of this omission in the institution's reporting behaviour.[174] The supervisory authority can subsequently reprimand the institution, including by imposing a formal measure.
FIU-NL may request further data or information following a report. This should be provided without delay.[175]

QA4.23: Question
Who should report unusual transactions?

Answer
It is important that unusual transactions are actually reported. Entities that do not have a compliance function can determine themselves which department Is responsible for reporting unusual transactions. If an entity has a compliance function the Wwft determined that this is responsible for reporting unusual transactions. As such, the compliance function must have the capacity, powers and resources to take on this responsibility.[176] This ensures that the unusual transactions are reported based on an independent evaluation.

The following principles should be applied when designing the reporting process:
- The decision to report should be made independently. This also means that other (first-line) priorities should not impede or affect the reporting process. The compliance function (if the entity has one) should have final say.
- The person responsible for implementing the reporting process should have sufficient capacity, powers and resources to do so.
- If the first line is responsible for (part of the) reporting process, reporting decisions must be justified to the compliance function (if the entity has one). Moreover, the employees involved should be able to carry out this part of their work independently and autonomously from the first line.

173 Section 16(2) of the *Wwft*. Section 16(5) of the *Wwft*: if it concerns a report filed under Section 16(4) of the *Wwft*, the institution must also explain why Section 16(4) of the *Wwft* applies.
174 Section 13, *under g*, of the *Wwft*.
175 Section 17 of the Wwft.
176 Section 2d(3) of the *Wwft*.

QA4.24: Question
What should an entity do with data on an unusual transaction?

Answer
Entities must retain records relating to unusual transactions. This includes:[177]

- The data provided by the entity to FIU-NL under Section 16(2) of the *Wwft* necessary to reconstruct the transaction in question.
- A copy of the report to FIU-NL, including any accompanying information and data.

FIU-NL's notice of receipt of the report.

QA4.25: Question
How long should an entity retain the data?

Answer
The retention period is 5 years from the time the report was filed or the time FIU-NL received it, respectively. The data must be easily accessible during this period.[178]

QA4.26: Question
Can an entity inform the customer about a report?

Answer
No. Entities and their employees may not disclose the fact that a report of an unusual transaction has been filed.[179] The customer to whom the report relates should also not be notified of it (the so-called tipping off prohibition), as this could potentially obstruct the investigation.

QA4.27: Question
Are there any exceptions to the duty of confidentiality?

Answer
Yes, there are. Exceptions arise from the law.[180]

The exceptions allow certain entities to share information on a report with entities that are part of the same group and, under strict conditions, with other entities belonging to the same category. In the latter case, the information sharing must relate to a customer of both entities and a transaction involving both entities, there should be equivalent confidentiality obligations and data protection, and the information sharing should be solely aimed at preventing money laundering and terrorist financing.

Without these exceptions, alert systems involving multiple entities could be less effective. The exchange of information must fit the purpose of the law and comply with legal requirements.

QA4.28: Question
Can a report of an unusual transaction be shared within the group?

Answer
An entity can share a report within the group unless FIU-NL has determined otherwise.[181]

177 Section 34(1) of the *Wwft*.
178 Section 34(2) of the *Wwft*.
179 Section 23(1) to (4) of the *Wwft*.
180 Section 23(5) and (6) of the *Wwft*.
181 Section 23a of the Wwft.

QA4.29: Question
Should an entity also file a police report if it suspects money laundering or terrorist financing?

Answer
In addition to notifying FIU-NL, an entity can also report any strong suspicions of money laundering or terrorist financing to the police at the same time.

QA4.30: Question
Should entities continue to report to FIU-NL if the Public Prosecution Service is requisitioning information?

Answer
Yes, they should. Entities may receive a requisition from the Public Prosecution Office to provide customer information as part of a criminal investigation into that customer (or third parties). The entity cannot share information relating to the requestion with their customer(s). The entity is still obligated to report unusual transactions.

QA4.31: Question
What happens when a report is filed with FIU-NL?

Answer
FIU-NL investigates reported transactions.[182] This investigation may result in a transaction being declared suspicious, in which case FIU-NL reports the transaction to the investigative authorities. Usually, the entity is notified of this.

GP4.25: Good practice - reporting procedure

An entity fully and immediately notifies FIU-NL of any proposed or executed unusual transactions. To this end, the entity has a procedure in place that defines the reporting process and what steps to take in case an unusual transaction is detected. The procedure also ensures that a report is filed as soon as the unusual nature of a transaction becomes known.

Part of the procedure is that 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 also reassessed.

GP4.26: Good practice - training programme

An entity provides sufficient guidance to its staff about reporting unusual transactions. It does so by discussing examples of cases on a quarterly basis and including this in the regular training programme.

GP4.27: Good practice - reporting based on objective indicator

An entity has set up an automated reporting process for transactions that match an objective indicator, which is periodically reviewed by the compliance function.

The process prevents the entity from potentially failing to report unusual transactions without delay and reduces the administrative burden.

182 I have reported an unusual transaction. What happens now? (fiu-nederland.nl)

GP4.28: Good practice - reporting transactions that have been reported to the police

An entity notifies FIU-NL of unusual transactions that it has reported to the police or the Public Prosecution Service in connection with money laundering or terrorist financing.

GP4.29: Good practice - confidentiality

An entity has policies and procedures in place that set out how it ensures confidentiality. This includes assigning appropriate access rights for core systems used to secure information flows and handle alert reports for unusual transactions.

It also includes periodically providing guidance and training to relevant staff, especially employees who interact with customers. It is essential that these employees are able to identify unusual transactions, what questions they have to ask the customer and what information they must not under any circumstances disclose to the customer.

4.1.6 Feedback and testing

A transaction monitoring system based on applied knowledge should fit the institution's risk profile (see also Section 4.1.1). This also means that the intelligence used must be dynamic: risks can change, and so can, for example, the business rules. In order to ensure that an entity continues to be able to identify risks and unusual transactions, it is important that the system and the applied knowledge are up to date. As new risks arise and old risks cease to be relevant, the institution's risk profile changes, which could mean that the transaction monitoring system needs to be adjusted as well.

Furthermore, certain business rules and models may stop being effective. This is the case if they generate too few true positives, too many false negatives or too many false positives. To determine whether this is the case, the transaction monitoring system must be tested and, if necessary, adjusted.

Q&A

QA4.32: Question
Does transaction monitoring need to be evaluated?

Answer
Yes, it does. An effective transaction monitoring system is an essential element in controlling the risk of involvement in money laundering or terrorist financing.

An entity should therefore periodically evaluate its system to assess whether the business rules and models applied are effective or ineffective. The latter could be the case, for example, if business rules are to loosely defined, or if they have thresholds and values that are too high or that do not fit the institution, resulting in very few alerts. By conducting periodic reviews, the entity can check whether certain business rules and models have failed to generate the alerts they should have generated, and whether adjustments may be necessary.

QA4.33: Question
Should advanced techniques also be tested?

Answer
Yes, they should. 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. This can be done, for example, by checking whether a model continues to perform well when it is used on a predetermined reference set.

QA4.34: Question
What is backtesting?

Answer
Business rules and models can be evaluated using backtesting. Based on the results of this, an entity 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:

1. Retrospective analysis of a selection of transactions which under a previous system configuration did not generate an alert. The aim of this is to assess whether the transaction monitoring 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).
2. An analysis of transactions which 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.
3. 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.
4. A retrospective analysis of the timeliness of notifications in order to improve this.

GP4.30: Good practice - testing business rules

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

GP4.31: Good practice - testing

An entity keeps its business rules and the settings of its transaction monitoring system up to date and tests them periodically. The entity documents these tests and the outcomes.

It also uses management information to monitor whether the output of the various business rules and models (e.g. in the form of numbers of alerts, FIU-NL reports and corresponding amounts) matches the risks identified in its risk analysis (SIRA). When the output of the institution's transaction monitoring system is too limited, the entity has insight into which business rules and models are inadequate with regard to detecting risks in the portfolio and whether additional measures need to be taken.

The entity documents the results of these analyses as well as the analysis process and any relevant considerations. The structural design of the quality assurance framework and periodic above- and below-the-line testing are also documented. Where necessary, the entity makes adjustments based on the results of the tests.

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

GP4.32: Good practice - feedback loop

An entity has a system in place to periodically evaluate the effectiveness of all its business rules that creates an overview of the variables that could potentially be used to make improvements. These variables are selected from a large set. During one of the periodic reviews, a business rule for international transactions with many more false positives for transactions within the EU than for transactions outside the EU has been identified.

The entity has supplemented this observation with a data and risk analysis to verify whether the envisaged risk is still fully covered by the business rule in the event of potential adjustments. The entity 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.

GP4.32: Good practice - using FIU-NL data and typologies

An entity has a procedure in place to ensure that its risk analysis is updated based on input from FIU-NL reports and FIU-NL feedback. Other sources, such as typologies and recent developments, are used to recalibrate the risk analysis as well.

Based on the updated risk analysis, the entity also reviews its business rules and models and adjusts these where necessary.

GP4.33: Good practice - identifying false negatives

Following a publication about a money laundering case, a bank checks payments made to a country in the Middle East. It finds that a 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 to ensure that these kinds of transactions do generate alerts in future.

4.2 Customer reviews

Customer reviews help entities keep their risk profiles and underlying data up to date. An entity can use a customer review to assess whether the customer still fits within its risk tolerance and whether additional measures are needed – or whether fewer measures will suffice.

Customer review can take place periodically or in response to an event, signal or alert. These alerts can come, for example, from transaction monitoring, changes in customer data and from external sources.

Q&A

QA4.35: Question
When is it important to conduct a review?

Answer
It is particularly important to conduct reviews for high-risk customers or if there are signs that a customer's risk profile has changed. A review must be conducted if:[183]

- there is an indication that the customer may be involved in money laundering or terrorist financing;
- the entity doubts the truthfulness or completeness of data previously submitted by the customer;
- it is justified to do so based on the risk that an existing customer may be involved in money laundering or terrorist financing.

The entity must take reasonable measures to keep the customer's records up to date.[184] The customer file must be updated in any case if there is a relevant change to the customer's circumstances. This includes conspicuous and anomalous transactional behaviour as well as changes to the customer's ownership or control structure. Signals the entity receives from, for example, the customer themselves or the press and legal cases also qualify as relevant changes.

QA4.36: Question
To what extent should a review involve customer contact?

Answer
The purpose of a review is to determine whether the customer's risk profile is still up to date, to update the customer's data where necessary, and to assess whether the level of control is still appropriate.
Depending on the risk and signals, the entity may suffice with consulting and analysing internal and external sources. Customer contact will not always be necessary.

QA4.37: Question
What should the result of a customer review be?

Answer
After a customer review, the entity should have an up-to-date and complete customer file that meets all the relevant requirements. The customer's risk profile should also be updated.

QA4.38: Question
What measures can an entity take following a review?

Answer
The outcome of the review may trigger the following measures:

- The entity parts with the customer. This primarily happens if:
  - The entity concludes, based on its customer review/customer due diligence, that the customer poses excessive integrity risks.

183 Section 3(5) of the *Wwft*.
184 Section 3(11) of the *Wwft*, Section 6(3) of the *Wwft*, Section 8(11) of the *Wwft*.

- The entity is unable (or no longer able) to determine exactly who the customer and/or the UBOs are, what the purpose of the business relationship is, or whether the intended service provision is appropriate. This can happen if customer due diligence (conducted as part of the customer review) is unsuccessful, for instance due to a lack of necessary information.[185]

- The entity tightens its controls for the customer or restricts it services.
- The entity relaxes its controls because the customer's risk profile is lower than before.
- If, based on the review, the entity determines that one or more unusual transactions have taken place, it reports these transactions to FIU-NL immediately after their unusual nature becomes known.[186]

QA4.39: Question

Must an entity terminate a customer relationship following a requisition by the Public Prosecution Service?

Answer

Entities may receive a requisition from the Public Prosecution Service to provide customer information as part of a criminal investigation. The entity cannot share information relating to the requisition with its customers.

A requisition may prompt the entity to conduct enhanced customer due diligence and additional monitoring of the customer's transactions. The outcome of the customer due diligence may lead the entity to implement additional controls or to report unusual transactions to FIU-NL (without discussing the requisition with the customer).

If, for the purpose of the investigation, the Public Prosecution Service does not want the customer to know that an investigation is ongoing, this will be explicitly stated in the requisition. This means that the customer must not be able to link any controls implemented by the entity to the Public Prosecution Service's investigation.

A requisition from the Public Prosecution Service does not have to be a reason for the entity to terminate the customer relationship under the *Wwft* or *Wft*, or to suspend its services. The entity may conclude, based on its customer due diligence, that the customer poses unacceptable risks and that there are grounds to part with the customer. If there are unacceptable risks or if customer due diligence requirements cannot be met, the entity should terminate the customer relationship at the earliest opportunity.

However, if the criminal investigation requires the continuation of the customer relationship and transactions, the customer relationship cannot be terminated. Any request to continue a customer relationship and transactions will be made by the prosecutor, upon requisition. 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. Entities may only part with a customer in cases like these if the Public Prosecution Service has given its permission.

185 Section 5(3) of the *Wwft*.
186 Section 16(1) of the *Wwft*.

GP4.35: Good practice - review

An entity carries out at least the following actions during a review:

- Check for sanctions and PEPs. For high-risk customers, a "bad press" check is also warranted.
- Analyse customer transactions, checking:
  - whether the transactions fit the purpose and nature of the relationship;
  - whether the transactions are plausible given the origin of the funds used in the relevant business relationship or transaction;
  - whether there are conspicuous transactions or transaction patterns (large amounts, unusually large cash transactions, amounts transferred immediately to another account, possible use of the accounts by third parties, unknown counterparties).
    Transactions that stand out and cannot be directly explained must be analysed in more detail. For the purpose of this analysis, further information should be obtained from the relevant customer if necessary, for example on the source of the funds.
- Update customer data, including UBO data.
- Update risk profile. This may affect the mitigating measures that need to be applied.

The entity has stipulated in its review procedure that the information collected should serve as substantiation for the analysis, risk profile and level of control.

GP4.36: Good practice - customer exit policy

An entity has drawn up a customer exit policy to ensure that relationships with existing customers are ended properly. Among other things, this policy states the circumstances under which the relationship with the customer will be ended, and the procedure for doing so (including time frames). The entity monitors exit processes and takes action if the agreed time frames are exceeded.

GP4.37: Good practice - additional information and exit

During customer review, an entity finds that one of its customers qualifies as a PEP. In response, the entity takes the additional measures set out in its policy and requests additional information. The customer refuses to provide this, whereupon the entity restricts its services and starts the exit procedure.

GP4.38: Good practice - restricting services

A bank finds that a customer is using their private banking account for business purposes. Based on further investigation and customer inquiries, the bank is unable to confirm the origin of the funds in the private banking account. The customer also has a payment account, which shows no potentially suspicious transactions.

The bank decides to close the private banking account, but not the payment account. The bank does tighten its controls for the payment account. This means, among other things, that payments above €2,000 are processed separately, and that they will be previewed and approved by the bank before further processing.

GP4.39: Good practice - relevant data

For each risk category, an entity has defined what data is relevant with regard to identified risks and how often the data in the customer file should be updated. The entity has set up its review procedure based on these definitions.

GP4.40: Good practice - determining frequency

The entity has defined its review frequency for each risk category. For lower-risk customers, the entity employs an event-driven review system. This means that the entity only conducts a review if there are signals (from internal or external sources, including transaction data and information gathered during customer interactions) that the customer's risk profile has changed or that the customer data is not up to date.

The entity has stipulated that a review must in any case be conducted if:

- the customer requests a new service or product;
- there are signs that the customer has moved to a high-risk jurisdiction;
- the customer becomes a PEP.

The entity has designed its operations (including its transaction monitoring) to ensure that relevant changes are detected in a timely manner. It regularly tests the effectiveness of this design, a process that is supervised by the compliance function.

For high-risk customers, the entity uses periodic reviews as well as event-driven reviews.

GP4.41: Good practice - agreements with customer

An entity has contractually stipulated that customers must report any board and shareholder changes without delay.

In addition, the entity has built a trigger into the system to identify board changes, using a link to the Chamber of Commerce database. For high-risk customers, the entity regularly checks whether the UBO information is still up to date.

Annex I – List of abbreviations

(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*)
BSN	Citizen service number (BSN)
CDD	Customer due diligence
EBA	European Banking Authority
EDD	Enhanced due diligence
eID	Electronic ID
eIDAS	Electronic Identities and Trust Services (regulation)
ETP	Expected transaction profile
FATF	Financial Action Task Force
FIU-NL	Financial Intelligence Unit
HRTC	High-risk third country
MiCAR	Markets in Crypto Assets Regulation
PPS	Public Prosecution Service
PEP	Politically exposed person
SIRA	Systematic integrity risk analysis
SME	Small and medium-sized enterprises
TFR	Transfer of Funds Regulation
UBO	Ultimate beneficial owner
Wft	Financial Supervision Act (*Wet op het financieel toezicht*)
WTR	Wire Transfer Regulation
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*)

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

Follow us on:

DeNederlandscheBank
EUROSYSTEEM