BFT
autoriteit voor
financieel-juridisch
toezicht

24 October 2024

Guideline on Compliance with the Money Laundering and Terrorist Financing (Prevention) Act

for accountants, tax consultants, administrative offices and all other institutions mentioned in Article 1a(4)(a) and (b) of the Act

Table of contents

This translation has been prepared with the utmost care. In the event of any discrepancies between the Dutch version of the Specific Guidelines and this translation, the Dutch version shall prevail.

1. Introduction

The Financial Supervision Office (in Dutch: BFT, autoriteit voor financieel-juridisch toezicht (BFT)) is the supervisory authority for compliance with the Money Laundering and Terrorist Financing (Prevention) Act (Wwft) for independent professionals, such as accountants, tax consultants and administrative offices (including payroll administration offices).[1] This Specific Guideline is intended for these professional groups.[2]

The Specific Guideline addresses points of consideration relevant to independent professionals in complying with the Wwft.[3] The Specific Guideline should be read in conjunction with the *Algemene leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)* (General Guideline on the Money Laundering and Terrorist Financing (Prevention) Act) issued by the Dutch Ministries of Finance and Justice and Security (General Guideline) (Dutch only).

The Wwft uses many open standards. The Specific Guideline explains how the BFT interprets and applies legal standards, and therefore constitutes a (partial) interpretation of those standards. The examples mentioned in this guideline are not exhaustive and are provided by way of illustration. If a specific situation or example is not described in the guideline, no conclusions should be drawn from it. An institution may also comply with the laws and regulations in a different way.

This guideline is not a legally binding document and does not replace laws and regulations.[4] The purpose of this guideline is to assist institutions under the BFT's supervision in applying statutory obligations. The General Guideline describes the general aspects of the Wwft that apply to all institutions.

Reading guide

The previous Specific Guideline from the BFT dates back to 24 October 2018. This new specific guideline has a different structure and is more aligned with the General Guideline. The main adjustments in the new specific guideline compared to the previous version can be summarised as follows:

- the decision was made to keep the guideline as concise as possible and to work with annexes that can be updated separately, offering more flexibility;
- a more thematic approach (topics: healthcare fraud, property fraud, cryptocurrency);
- addition of more practical examples, both regarding customer due diligence (e.g., determining the Ultimate Beneficial Owner) and the obligation to report unusual transactions (practical examples for various groups based on case law and supervisory practice);
- updating of the examples for the subjective indicator based on recent case law and insights.

[1] Article 1a(4)(a) and (b) of the Wwft.
[2] The BFT has drawn up a separate specific guideline for institutions falling under Article 1a(4)(d) and (e) of the Wwft.
[3] This Specific Guideline integrates the previous specific guidelines (2018, 2014 and 2011) and other published interpretations and statements from the BFT. The relevant legislative changes compared to the specific guideline issued in 2018 are included in Annex **3**.
[4] This Specific Guideline is not a policy rule as referred to in Article 1:3(4) of the General Administrative Law Act (*Algemene wet bestuursrecht*).

The Specific Guideline covers several topics. These are summarised below:

Subject	Chapter
Wwft principles	2
Wwft supervision	3
General Wwft obligations	4-6
Customer due diligence	7
Monitoring obligation	8
Obligation to report unusual transactions	9
Sanctions Act	10
Other topics	11-12

2. Wwft principles

2.1 General

The Wwft aims to combat money laundering and terrorist financing to safeguard the integrity of the financial and economic system. Customer due diligence and the obligation to report unusual transactions form the core of the Wwft – in addition to the general obligations.

The Wwft generally follows a principle-based and risk-based approach. However, it also imposes obligations on institutions where there is no room for a risk-based approach. Institutions must fully comply with these obligations. An example is the requirement to conduct customer due diligence. The Wwft specifies what the customer due diligence must achieve, but it is up to the institution to determine how to achieve this result. Conducting customer due diligence contributes to identifying and managing the risks that certain customers or types of services may pose. The risk-based approach means that an institution must tailor the measures of customer due diligence to the risk associated with a specific type of customer, relationship, product or transaction.

Compliance with the Wwft obligations is essential for an institution to effectively fulfil its role as a gatekeeper. This Specific Guideline emphasises the purpose of the Wwft.

An institution engaged in business activities covered by the Wwft is expected to be aware of the applicable laws and regulations[5]. In addition, a certain level of expertise is expected from the institution in the area in which it operates[6].

2.2 What is money laundering?

Money laundering has several definitions. Generally speaking, money laundering can be described as the mixing of illegal financial flows with legal financial flows, with the aim of giving the illegal financial flows legal status.

Article 420bis of the Dutch Penal Code reads as follows:
"1. Being guilty of money laundering shall be punishable [...]*:*

[5] See also: ECLI:NL:RBDHA:2016:13678.
[6] See also: ECLI:NL:RBDHA:2016:11828.

a. he who conceals or disguises the true nature, origin, location, disposition or movement of an object, or conceals or disguises who is the rightful owner of an object or has it in his possession, while knowing that the object - directly or indirectly - originates from any crime;

b. he who acquires, possesses, transfers or converts an object or uses an object, while he knows that the object - directly or indirectly - originates from any crime.

2. Objects mean all items of property and all property rights."[7]

An institution does not need to assess whether it meets the description of the offence in the Dutch Penal Code. After all, it must report a transaction if it has reason to suspect that it **may** be linked to money laundering (unusual transaction).

The European Directive on combating money laundering by criminal law[8] includes a list of criminal activities that serve as predicate offences for money laundering. This directive is relevant for institutions, as it specifically names offences that can be regarded as predicate offences for money laundering.[9]

Examples of (relevant) criminal activities in this Directive are:
- terrorism;
- illegal trafficking in narcotic drugs and psychotropic substances;
- corruption;
- fraud;
- environmental crime;
- tax crimes related to direct and indirect taxes;
- insider trading and market manipulation;
- cybercrime.

Stages of money laundering

The various methods of money laundering typically involve three stages[10]:

1. Placement: the process of introducing criminal proceeds into the financial system.

   In this stage, cash proceeds from criminal activities are made electronic. This can happen in a direct or indirect manner. In the direct method, cash proceeds are deposited into a bank account.

   In an indirect method, for example:
   - criminal money is attempted to be channelled through a third-party account of a gatekeeper; or
   - straw men and/or companies are used as covers.

2. Layering: the process of layering financial transactions to obscure the criminal origin of the funds.

   In this stage, the criminal attempts to conceal the origin of criminal money by engaging in multiple financial transactions or stacking them. For example, by frequently transferring funds, withdrawing

[7] Money laundering is independently punishable under Articles 420bis, 420bis(1), 420ter, 420quater, 420quater(1) and 420quinquies of the Dutch Penal Code.
[8] Directive (EU) 2018/1673 of the European Parliament and the Council of 23 October 2018 on combating money laundering by criminal law.
[9] For the sake of completeness, the BFT notes that the activities mentioned were already considered predicate offences for money laundering prior to the implementation of Directive (EU) 2018/1673.
[10] J.L.S.M. Hillen, Schuurman & Jordens, *integriteits- en anti-witwaswetgeving* (integrity and anti-money laundering legislation), 2004 third edition, *introductie bij de Wet Mot* (introduction to the Disclosure of Unusual Transactions (Financial Services) Act), pages 132 and 133.

them, splitting them or entering into sham loans or fictitious contracts. These actions break the paper trail.

3. Integration: the process of integrating the funds into the legal economy.

   In the integration phase, criminal proceeds are used, for example, to purchase luxury goods. Integrating criminal funds into the legal economy can also manifest itself in activities such as purchasing and/or selling shares or immovable property.

Examples of money laundering and unusual transactions can be found here (Dutch only).

The reporting obligation is low-threshold. An institution does not need to determine itself whether money laundering has occurred in a criminal sense or whether the three stages of the money laundering process have been fulfilled. It is sufficient for an institution to identify unusual transactions and report them to the Financial Intelligence Unit of the Netherlands (FIU-NL)[11].
In assessing whether or not to report an unusual transaction, the materiality applied by accountants does not play a role.

Money laundering methods and threats

The Dutch NRA on Money Laundering (2023)[12] describes money laundering threats. According to the NRA, the greatest threats in the area of money laundering are:

Money laundering via
criminal underground banking or hawala banking
easily accessible ways to open a foreign bank account
trade-based constructions involving goods or services
the purchase/sale, rental or lease of high-value products
foreign (offshore) structures
a the physical movement of large amounts of cash and/or high-value products in the Netherlands or to/from abroad
less transparent Dutch legal structures
professional service providers
financial crypto service providers
straw men, front men or money mules
Payment Service Providers
transactions from, to or via foreign bank accounts
commercial real estate
splitting up trust office services
private real estate
licensed money transfer organisations
wire transfers at licensed banks
cash transactions/deposits at licensed banks

Source: Dutch central government - WODC

[11] See also: ECLI:NL:CBB:2015:363.
[12] NRA stands for National Risk Assessment. This is conducted by the Ministry of Justice and Security's Scientific Research and Documentation Centre (WODC).

2.3 What is terrorist financing?

Terrorist financing is essentially a collective term for various actions that ultimately aim to financially enable terrorist activities.

Terrorism is defined as the execution of violence (or the preparation thereof) aimed at human lives or causing societal disruption, driven by ideological motives, with the goal of instilling severe fear all or part of the population, bringing about societal change and/or influencing political decision-making.[13] [14]

In the NRA on Terrorist Financing for the Netherlands (2023), the following forms of terrorism are mentioned:

- religiously motivated terrorism;
- right-wing extremist motivated terrorism;
- left-wing extremist motivated terrorism;
- nationalist and separatist motivated terrorism; and
- single-issue motivated terrorism.

For the purposes of the Wwft, terrorist financing is considered to be:

"anyone who intentionally provides themselves or another with funds or information, or intentionally collects, acquires, possesses or provides to another, funds or items that wholly or partially, directly or indirectly, serve to provide financial support for the commission of a terrorist crime or a crime in preparation for or facilitating a terrorist crime."[15]

This definition shows that terrorist financing occurs even if the funds and/or other assets are not actually used to commit terrorist acts or are not directly related to terrorist acts.

The reporting obligation is low-threshold. For the reporting obligation under the Wwft, an institution does not need to determine whether terrorism has actually occurred. It is sufficient for an institution to identify unusual transactions and report them to FIU-NL.
In assessing whether or not to report an unusual transaction, the materiality applied by accountants does not play a role.

Examples of terrorist financing can be found here (Dutch only).

The NRA on Terrorist Financing for the Netherlands (2023) describes threats in the field of terrorist financing. According to the NRA, the greatest threats in the area of terrorist financing are:

Financing via/with
unlicensed money transfer organisations and hawala banking
easily accessible (online) ways to open a foreign bank account
the physical movement of (large amounts of) cash or highvalue products in/via the Netherlands or to/from abroad
legally obtained own resources
crypto service providers
funds obtained via a form of crime other than fraud
foundations with little transparency about finances and no self-regulation

[13] Source: General Intelligence and Security Service (AIVD).
[14] Article 83 of the Dutch Penal Code specifies which punishable conducts are considered terrorist crimes. Article 421 of the Dutch Penal Code criminalises terrorist financing.
[15] Article 421(1)(a) of the Dutch Penal Code.

donations through payment requests and/or crowdfunding through social media
internet payment services (Payment Service Providers, PSPs)
wire transfers or cash transactions at licensed money transfer organisations
funds obtained via horizontal/vertical fraud
wire transfers or cash transactions at licensed banks

Source: Dutch central government - WODC

2.4 Difference between money laundering and terrorist financing

The difference between money laundering and terrorist financing lies mainly in the origin and destination of the money. In money laundering, the origin of the money is by definition illegal, and the goal is to find a legal use for it. In terrorist financing, this is often the opposite. The funds are used for criminal purposes, but the origin can be either legal or illegal. For financing terrorist acts, the same channels are often used as in the case of money laundering.[16]

2.5 What is a transaction?

A transaction under the Wwft is an action or set of actions by or for the benefit of a customer that an institution has become aware of in connection with its services to that customer.

An unusual transaction falls under the reporting obligation if the following two conditions are met. It concerns a transaction:

- that an institution has observed in connection with its services;
- 'by or for the benefit of a customer'.

The Trade and Industry Appeals Tribunal (CBb) calls 'by or for the benefit of a customer' in short 'involvement of a customer'[17]. It must concern a transaction in which the customer of an institution is involved. Active involvement of the customer (i.e. the customer performing an action that may indicate money laundering) is not required; passive involvement is sufficient.

Passive involvement occurs if:

- someone other than the customer performs an action;
- that action may indicate money laundering by that other person; and
- the customer is aware of this. The customer explicitly or implicitly agrees. The customer thus becomes a party to that action.

In 2022, the Court of Amsterdam further explained[18] 'actions by or on behalf of the parent company' as part of the transaction concept. The question was whether a transaction carried out by a subsidiary also counted as a transaction by or on behalf of the parent company.
The direct or indirect involvement of the parent company in the actions must have been significant enough to be considered a joint planning and execution. Alternatively, the transaction must have been carried out specifically for the benefit of the parent. This must be assessed on a case-by-case basis. An example of direct/active involvement is a transaction initiated by the parent company. There can also be indirect/passive involvement, where the subsidiary initiates the transaction, but the parent company was involved in, for example, the decision-making process of the transaction or approved the transaction. Consolidation alone does not imply that the subsidiary and the customer/parent company can be considered the same entity, as was the case in the CBb ruling[17].

[16] Dutch House of Representatives, session year 2007-2008, 31238, number 3, page 2.
[17] See also: ECLI:NL:CBB:2018:6, legal ground 3.5.
[18] See also: ECLI:NL:RBAMS:2022:7570.

In 2024[19], the CBb ruled in a case where an accountant was tasked with auditing consolidated financial statements. The unusual transactions, which had come to light following questions about the current account position with the parent company, were part of a foreign subsidiary.

In its decision of 3 September 2024, the CBb considered as follows:
"5.3. The Tribunal is of the opinion that this indeed concerns actions by the customer or by a third party on behalf of the customer. As the Accountancy Division rightly considers, the accountant became aware of the unusual transactions because they discovered a current account discrepancy while auditing the consolidated financial statements of [name 2] and raised questions about it. Transactions were carried out from [name 3] on behalf of [name 2]. Because [name 3] is part of the group, these transactions influence the consolidated financial statements of [name 2]. Therefore, these are actions by the customer or by a third party on behalf of the customer. The fact that [name 3] operates as an independent entity does not change this.
5.4. The Tribunal further considers that Article 16 of the Money Laundering and Terrorist Financing (Prevention) Act (Wwft) does not require a connection to the Netherlands for the reporting obligation. [...] The consolidated financial statements of [name 2] are an account for all transactions belonging to the [name 11], so for this reason, there is already a connection to the Netherlands."

Actions between third parties where the customer is not involved do not fall under the definition of a transaction within the meaning of the Wwft. These do not need to be reported, unless they are transactions by or on behalf of the customer.

2.6 Available Wwft information

The BFT provides information regarding the Wwft through its website. If there are any legislative or interpretive changes after the publication date of this Specific Guideline, they will be published on the BFT website.

The Financial Action Task Force (FATF)[20] publishes information and recommendations relating to money laundering and terrorist financing on its website.

The Anti Money Laundering Centre (AMLC) publishes on its website information related to money laundering, money laundering techniques and money laundering indicators.

FIU-NL sends various messages to business contacts: alerts, instructions and knowledge updates. FIU-NL's website includes an explanation of how to report unusual transactions and includes real-life cases for each reporting group.
In addition, FIU-NL's website includes various money laundering typologies (Dutch only).

Various professional and industry organisations inform their members about the obligations under the Wwft as well as relevant case law. They also answer members' questions about practical situations.
The guidelines of the Dutch Association of Tax Advisers (NOB), the Royal Netherlands Institute of Chartered Accountants (NBA) and the Dutch Register of Tax Advisers (RB) are available to everyone.

[19] See also: ECLI:NL:CBB:2024:616.
[20] The FATF is an intergovernmental organisation. The goal of the FATF is to prevent and combat money laundering, terrorist financing and the financing of weapons of mass destruction in order to ensure the integrity of the international financial system. To this end, the FATF has established 40 standards. Countries are expected to implement these standards in their laws, regulations and policies.

3. Wwft supervision

3.1 General

The BFT has been designated as the supervisory authority compliance with the Wwft for independent professions under Article 1d(1)(c) of the Wwft.

For this Specific Guideline, it concerns supervision of the professions listed in Article 1a(4)(a) and (b) of the Wwft. This includes natural persons, legal entities or companies that work as tax consultants, external registered accountants or external accounting consultants, explicitly listed as institutions.

However, these articles also refer to **similar activities**. Therefore, other independent professions may also fall under the scope of the Wwft (see Sections 3.3 and 3.4).

To fall within the scope of the Wwft, the activities must be carried out **independently and autonomously**. This applies when the professional is not in a hierarchical relationship, as is the case with employees, and when the professional performs the activities without being under the responsibility of another institution.

In addition, the activities must be carried out on **a professional or business basis**. This means that:

- the service is not provided only incidentally; and
- the provider (typically) receives remuneration[21] or generates income.

Occasional or one-time activities are insufficient to qualify as professional or business activities. However, it is not important whether the activities are profitable or whether they are the primary activity of the professional.

Exemption under the Wwft

Tax consultants and other professionals providing similar services **do not** fall under the scope of the Wwft when they perform work for a customer that relates to:

- determining the legal position of that customer;
- its representation and defence in legal proceedings;
- providing advice before, during and after legal proceedings; or
- initiating or avoiding legal proceedings.

Determining the legal position typically occurs during the first (exploratory) conversation. During this conversation, the Wwft does not yet apply. However, in complex cases, it may take more time and analysis to determine which services are needed. This could lead to an assignment following the exploratory conversation. If this assignment is related to determining the legal position, the Wwft still does not apply. When it becomes clear which activities need to be performed for the customer, the institution must reassess whether these fall under the exemption of the Wwft.

It is important for an institution to be aware that for any other services provided to this customer, the Wwft obligations may still apply.

[21] Remuneration can also be in kind, for example, when a service provided by the institution is exchanged for a service from its customer.

3.2 Administrative offices

As previously mentioned, the Wwft defines which professional activities are subject to the law through the concept of 'institution'.

The explanatory memorandum[22] clarifies that for the scope of Article 1a of the Wwft, the nature of the activities performed is decisive, not the entity performing the service. The explanatory memorandum includes the following:

"In the definition of accountants and similar professionals, a change has occurred. The definition in this proposal aligns with the amended definition in the Third Money Laundering Directive, which states that these institutions fall under the scope of the directive if they perform activities «in the context of professional activities». This refers to activities such as tasks related to financial statements, bookkeeping, tax advice, completing tax returns […]*".*

The mentioned professional activities can also be carried out by administrative offices, as stated in the General Guideline. Therefore, administrative offices are also considered institutions under the Wwft. Administrative offices are thus also subject to the supervision of the BFT.[23]

To be considered an institution, only the nature of the activities is relevant, not the scale.

3.3 Payroll administration offices

Depending on the services offered by payroll administration offices, they may also fall under the Wwft and therefore under the supervision of the BFT.

An overview of this is provided in the table below.

Matrix application of the Wwft

Activities/services	Wwft applicable?	If yes, which article?
Processing salary data, changes and preparing payslips	yes	Article 1a(4)(b)
Processing salary data, changes, preparing payslips and submitting payroll tax returns	yes	Article 1a(4)(a) and (b)
Paying out salaries	no	
Providing software for payroll calculation	no	
Advice on payroll tax issues	yes	Article 1a(4)(b)
Advice on HR matters without tax services	no	

3.4 Supervision and assessment arrangements

The BFT collaborates with various professional and industry organisations. When a collaboration takes on a more structural form, the BFT aims to establish an arrangement. The BFT has established assessment arrangements with the NBA and the RB, and a supervision arrangement with the SRA.

This means that the BFT will initially refrain from conducting 'regular' investigations at the members of these organisations. A regular investigation means that there are no prior indications or signals suggesting that there could be potential violations of the Wwft.

[22] House of Representatives, session year 2011-2012, 33238, number 3, page 7.
[23] See also: ECLI:NL:RBAMS:2019:8873.

The BFT retains the possibility to conduct 'special' investigations. This means that the BFT has a clue or signal regarding an institution or its customer.

The BFT also conducts partial investigations into specific Wwft obligations, such as risk policy and management, compliance and/or audit functions, training obligations and screening obligations. These partial investigations are carried out within all professional groups under the BFT's supervision. The goal is to gain insight into how this specific statutory obligation is handled within the various professional groups. These are not regular investigations as defined in the various arrangements that the BFT has established.

4. Risk policy and management

4.1 General

Certain types of customers or products can carry an inherent increased integrity risk. These increased inherent risks can be mitigated by taking appropriate measures. The Wwft thus follows a risk-based approach: an institution must align its procedures with its own Wwft risks. This means that the intensity of the (mitigating) actions depends on the risk assessment: the higher the risks, the more effort is expected from an institution to mitigate those risks. It is important for institutions to establish guidelines to support risk assessment.

The General Guideline explicitly states that the Wwft does **not** imply that customers with inherently high risks may be categorically rejected. Of course, an institution may decide which customers it accepts based on its customer acceptance and risk policy. This may lead an institution to decide to serve customers with an inherently higher risk. It is the institution's own responsibility to assess the relevant risks and then implement sufficient mitigating measures accordingly.

In the context of the Wwft, a distinction can be made between risk policy and risk management. An institution generally has its own rules regarding which customers are and which customers are not accepted. This is part of the risk policy.

This means that if an institution chooses to offer services or serve customers with a higher risk of money laundering or terrorist financing, it must take additional measures to manage these higher risks. This is part of risk management.

The General Guideline emphasises that in all cases it is important that the risk selection of institutions is made on non-discriminatory grounds.

4.2 Identification and management of risks

The Wwft requires institutions to establish and maintain an up-to-date written risk policy. A **written** risk policy is therefore always mandatory. It is important for the risk policy to be tailored to the institution's organisation and customer portfolio. It is conceivable that institutions assess risks differently in similar cases.[24]

For example, a small office with one employee may be required to establish a less detailed risk policy than a larger office. An office with only local SMEs as customers may need to establish a less detailed risk policy than an office with an international customer portfolio.

[24] Guiding and setting up an international structure (with entities from different countries) need not be a high risk for a specialised firm in itself. A tax consultant who does not deal with this on a daily basis may assess it differently.

The risk policy involves institutions setting behavioural guidelines, procedures[25] and measures. They must at least comply with the requirements set by the Wwft in the following areas:

- risk management;
- customer due diligence;
- obligation to report unusual transactions;
- retention of supporting documents; and
- training and screening.

The policies, procedures and measures must be approved by a policymaker.

The BFT considers risk policy and management to be of great importance for correct compliance with the Wwft. According to the BFT, the risk policy and management must at least meet the following requirements:

- risk policies and management are based on the most recent Wwft, are regularly updated and are sufficiently concrete and implementable;
- the risk policy provides insight into high-risk customers and transactions, both at the time of entering into the customer relationship and during the course of the customer relationship;
- the risk policy must demonstrate when there is a higher risk of money laundering and/or terrorist financing;
- the risk policy must show what measures the institution must take to manage these risks;
- risk management must provide staff with tools to manage higher risks.

In the risk assessment, an institution must at least consider the following risk factors:

- the type of customer;
- the type of product;
- the service or transaction involving the customer;
- the delivery channels used by the customer; and
- the countries or regions with which the customer does business.

An institution is expected to assess the risks of money laundering and/or terrorist financing for each customer/transaction and document the outcomes. For one thing, the Wwft requires institutions to make use of the most recent versions of the supranational risk assessment[26] and the NRAs on money laundering and terrorist financing.

After an institution has identified the risks, it must take measures to manage them. This means, in line with the monitoring obligation, that there must be continuous monitoring to check whether the measures in place are effective. If the risks are too high and cannot be adequately managed, it may mean that an institution must discontinue its relationship with a customer.

An institution can incorporate the risk policy as part of the systematic integrity risk analysis (SIRA).[27]

[25] Annex 2 to the Specific Guideline contains a 10-step Wwft plan (Dutch only).
[26] The 'Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities' (2022) is a publication of the European Commission.
[27] See also *Handvatten bij toepassing Systematische Integriteitsrisico Analyse (SIRA)* (Guidelines for the application of Systematic Integrity Risk Analysis) by the Dutch Authority for the Financial Markets (AFM) and *SIRA van analyse naar beheersing* (SIRA from analysis to control) by the AFM and the BFT (both Dutch only).

5. Audit and compliance function

5.1 General

An institution can have different levels in which the compliance with laws and regulations is ensured, also known as the three lines of defence.

The **first** line consists of the employees responsible for providing services and the internal control system they apply. For example, procedures that employees use to establish and verify the identity of customers (or potential customers).

The **second** line is the compliance function. This monitors whether the institution's daily practices are in accordance with internal procedures, measures and agreements, as well as with statutory provisions.

The **third** line is the audit function. This is responsible for periodically evaluating the effectiveness of the organisational structure, the procedures and measures integrated into the institution's business processes, and the compliance function.

The compliance function focuses on ensuring compliance with the Wwft obligations, including reporting to FIU-NL. The audit function checks the compliance of the executed compliance function.
The three-lines-of-defence model contributes to effective risk management, particularly in larger organisations.

Compliance function

The compliance function must be carried out independently and effectively. In principle, this means that the individuals involved in the compliance function may not be involved in the activities they supervise.[28] This separation of functions is important to promote effective compliance.

Audit function

The audit function must be independent. In principle, this means that the individuals involved in the audit function may not be involved in the activities they supervise, meaning they may not be involved in compliance or in the primary process.

An institution may choose to outsource the compliance function and the audit function (either fully or partially). This is not mandatory. The audit function can also be performed by an internal auditor[29].

5.2 When is it mandatory?

The establishment of an independent compliance and audit function is made mandatory for Wwft institutions, insofar as it is appropriate to the nature and size of the institution[30]. According to Article 2d(1) of the Wwft, this obligation only applies if the day-to-day policy of the Wwft institution is determined by two or more persons.

---

[28] Dutch House of Representatives, session year 2017-2018, 34808, number 3, page 44.
In exceptional cases, it may occur that the compliance officer himself is also involved in the execution of the primary activities. If there are Wwft compliance issues with the compliance officer's own customer, a discussion must take place with a deputy compliance officer who is not involved in the case to ensure the independence of the compliance function.

[29] With regard to the audit function, the 2018 Specific Guideline included: *"In outsourcing, this could include, for example, the audits conducted by the SRA or the NBA quality assessments. For designated RB members, the RB assessment may play a role. The external auditor can also fulfil the role of the audit function."* According to the BFT, the regular reviews do not sufficiently fulfil the audit function as referred to in the Wwft.

[30] Article 2d of the Wwft.

The Wwft supervisory authorities may provide guidance to support this.[31] A reasonable application of the law implies that a compliance and audit function must at least be mandatory for businesses that are required by the Dutch Works Councils Act (WOR) to have a works council. This typically applies to businesses with a total workforce of 50 or more employees[32].

An institution is expected to fulfil the compliance function at least annually.
The intensity of the implementation of the audit function must be tailored to the risk profile of the institution.[33] If there are indications that the compliance function is not functioning properly, this may justify more frequent use of the audit function. For institutions that have an audit function on other grounds, there is the possibility of including Wwft obligations in their audits.

In practice, partnerships often exist between, for example, accountants and tax consultants or civil-law notaries and tax consultants. If the partnership has a workforce of 50 employees or more, a compliance and audit function is mandatory.

Given the *nature* of the business, a compliance and audit function may also be mandatory at institutions with fewer than 50 employees. If an institution's risk policy shows that more than 75% of its customers or transactions have a high-risk profile, the institution is required to set up a compliance and audit function. This may be the case if a small tax advisory firm advises object companies from the trust sector or prepares tax returns for them. This is not expected to occur frequently in practice.

5.3 Assessment framework for compliance and audit functions

5.3.1 Preconditions

For an effective implementation of the compliance and audit functions, it is essential that the individuals performing these functions have sufficient expertise, authority and resources, and have access to all necessary information.

5.3.2 Content of the Wwft compliance function

When establishing the Wwft compliance function, the following tasks can be considered:

- monitoring Wwft office procedures;
- involvement in customer acceptance, particularly with respect to integrity risks of customers (or potential customers) of the institution.
  Examples include tax evasion and other forms of fraud, avoiding sanctions legislation, money laundering practices or terrorist financing;
- reporting findings to the institution's board (e.g. on the number of reports, high-risk cases);
- active involvement in the Wwft risk policy and management;
- active monitoring role in serving high-risk customers;
- keeping relevant employees' knowledge of the Wwft up-to-date. For example, by providing internal courses and explaining legislation to employees;
- informing employees about internal standards, office procedures and measures;
- providing advice to employees on whether in certain cases a transaction must be classified as unusual;
- ensuring the reporting of unusual transactions to FIU-NL. If a decision is made not to report, the reasoning behind this decision must be documented and kept on record;
- acting as a point of contact for supervisory authorities in case of inquiries or investigations.

[31] Dutch House of Representatives, session year 2017-2018, 34808, number 6, page 44.
[32] The BFT advises institutions to keep a fixed reference date, for example January 1 of any year.
[33] House of Representatives, session year 2017-2018, 34808, number 3, page 45.

5.3.3 Content of the Wwft audit function

When establishing the Wwft audit function, the following tasks can be considered:

- evaluating the effectiveness of the organisational structure;
- evaluating the effectiveness and completeness of business processes and office procedures;
- evaluating the effectiveness of the compliance function by reviewing whether the compliance officer has carried out their duties adequately in individual cases.
  Example: checking whether the reports made by the compliance officer are complete and accurate and whether, in certain cases, it was appropriate to refrain from reporting;
- reporting findings, including any identified deficiencies or non-compliance, to the management of the institution.

6. Training, education and qualification

6.1 Training obligation

To properly fulfil the gatekeeper role, it is crucial that an institution complies with the training obligation as outlined in Article 35 of the Wwft. An institution must ensure that its employees and day-to day policymakers are familiar with the provisions of the Wwft. To keep up with developments and continually raise awareness, training is not a one-time event but must be offered periodically (regularly). The training must be tailored to:

- the size of the organisation;
- the services offered; and
- the risk assessment of the customer portfolio.

An institution must be able to conduct customer due diligence properly and completely. Furthermore, employees and day-to-day policymakers must be aware of and stay updated on potential (new) forms of money laundering and terrorist financing so that unusual transactions can be identified.

To make the training as effective as possible, it is important to tailor the training offered to the different roles within the institution. For example, the content, depth and frequency will depend on the position the employee holds. For instance:

- the person responsible for the compliance function will receive additional, more in-depth training to stay up-to-date on developments in laws, regulations, and money laundering and terrorist financing risks.
- the day-to-day policymakers will receive sufficient training to meet their (ultimate) responsibility for ensuring compliance with the Wwft.

The implementation of the training obligation is an open standard. This means that the training obligation can be fulfilled through certified training programmes, (in-house) training, (online) courses, technical consultations, and studying guidelines and directives (or a combination of the foregoing). It is advisable for an institution to establish a training plan outlining how the various functions within the organisation, or individual employees, will meet the training obligation.

Simply regularly discussing specific Wwft-related matters during team meetings cannot be considered periodic training in the sense of Article 35 of the Wwft.[34]

[34] See also: ECLI:NL:CBB:2020:120.

It is the institution's responsibility to demonstrate that the training obligation has been concretely fulfilled. Adequate documentation of the training offered, the training attended, the frequency and the employees who participate in the training allows the institution to continuously assess, monitor and respond to the level of knowledge within the organisation.

6.2 Screening obligation

From 15 October 2020, under Article 35 of the Wwft, an institution must ensure that its employees and day-to-day policymakers, are screened. According to the explanatory memorandum to the amendment to the Wwft, screening relates to the risk of an institution being misused for money laundering and/or terrorist financing. The screening must be tailored to the employee's or policymaker's duties, as well as the risks, nature and size of the institution.

The FATF recommends that an institution must have adequate screening procedures in place to ensure high standards when hiring (new) employees.

The screening authority Justis has published a brochure providing guidelines.

Examples of tasks that an institution can carry out include:

- identity verification based on an original identity document;
- obtaining a copy of a bank card;
- pre-employment screening and in-employment screening (possibly supplemented with performance reviews or periodic evaluation interviews);
- integrity questionnaire;
- disclosure of functions (including ancillary functions);
- implementing a code of conduct;
- (periodically) requesting a Certificate of Good Conduct (VOG);
- reviewing CVs and references, checking at least the past three years;
- verifying diplomas and transcripts based on original documents;
- searching for information through the Internet;
- checking if the employee or policymaker is listed on sanction lists, particularly Dutch, European and UN sanction lists;
- checking if the employee or policymaker is a PEP (Politically Exposed Person).

It is important that an institution implements control measures when, based on the screening, it has identified a higher risk.

7. Customer due diligence

7.1 General

The Wwft only specifies what the outcome of the customer due diligence must be. However, the Wwft sets some conditions for customer due diligence, which are primarily focused on the intended goal (principle-based). The institution has a **result obligation** for customer due diligence: the institution must complete all aspects of the customer due diligence with sufficient results.

Customer due diligence is extensively discussed in the General Guideline. In this Specific Guideline, some additional points of consideration are discussed.

7.2 Customer due diligence obligations

7.2.1 Content and obligations of customer due diligence

Customer due diligence must be demonstrably tailored to the risk of money laundering or terrorist financing associated with the type of customer, business relationship, product or transaction.

In practice, the BFT observes, particularly at smaller institutions, that merely identifying the customer and verifying their identity is considered sufficient. However, the (standard) customer due diligence must include the following tasks:

- identifying the customer and verifying their identity using a document designated for that purpose;
- mapping and understanding the ownership and control structure of the customer;
- if the customer is not a natural person, identifying the Ultimate Beneficial Owner (UBO) of the service provided and taking reasonable measures to verify their identity;
- determining the purpose and intended nature of the business relationship;
- monitoring (ongoing tracking) of the risk profile based on its own risk policy;
- recording and retaining the associated data in a file for five years after the transaction or the termination of the customer relationship, unless a statutory provision states otherwise.

These tasks must always be performed. There is no distinction here between simplified, standard and enhanced customer due diligence. Only the depth of the due diligence varies. For enhanced customer due diligence, additional requirements apply (see Section 7.4).

The general rule is that an institution must identify the customer (and any UBO) and verify the customer's identity (in person) before providing services. Timely verification also applies to the UBO's identity. The intensity of verifying the UBO's identity can be adjusted based on the risk of the customer or transaction. The verification of the UBO's identity does not necessarily need to be done in person in all cases.

7.2.2 Identifying the customer and verifying their identity

7.2.2.1 Data from a reliable and independent source

An institution must establish and verify the identity of the customer. During the identification process, the customer provides information about their identity. During verification, the institution must verify whether the identity provided by the customer matches their actual identity.

Verification of identity must be based on documents, data or information from a reliable and independent source[35].

In practice, the BFT observes that some (particularly smaller) institutions use copies of Chamber of Commerce extracts or identity documents provided by the customer or third parties. A copy of a Commercial Register extract or an identity document obtained from a third party is not considered data from a reliable source.

An exception to this is an institution that uses the options provided by the Wwft to have the customer due diligence carried out by a third party or to adopt the customer due diligence of another Wwft institution[36].

[35] Article 11 of the Wwft. See also Article 4(1) of the Wwft Implementing Regulations for an overview of the documents that can be used for this purpose.
[36] Article 10 of the Wwft and Article 5(1)(a) of the Wwft, respectively.

7.2.2.2 Necessary data for verification

For the documentation of verification data, the following applies. While an institution may retain a copy of the identity document under the Wwft, it is not necessary for the institution to have a copy of an identity document in the (customer) file to comply with the Wwft[37]. However, the institution must have the necessary data[38]:

What/Who	What data/documents
Natural persons (no UBO)	– Surname, first name, date of birth, address and place of residence, or a document with person identifying number (and with which the identity has been verified); and – Type, number, date and place of issuance of the document used to verify identity. – If the customer is represented by a natural person: place of establishment of the customer + the above-mentioned details of that natural person.
Natural persons, who are UBOs	– Identity of the UBO (i.e. at least surname and first names); and – The data and documents gathered based on reasonable measures taken to verify the identity of the UBO.
Companies or other legal entities	– Legal form, name given in the articles of association, trade name, address with house number, postal code, place of establishment and country of registered office. – If applicable: registration number with the Chamber of Commerce and the method of identity verification. – Surname, first names and date of birth of those acting on behalf of the company or legal entity.
Trust or other legal constructs	– Purpose and nature of the trust or other legal construct; and – The law by which the trust or other legal construct is governed.

Source: General Guideline

7.2.2.3 Remote identification and verification

An institution may verify the identity of customers remotely where appropriate. The Wwft stipulates that verification must be based on 'sufficiently reliable means'. For example, an eID method[39] or two-way audiovisual tools (such as MS Teams, Skype, FaceTime).

Remote verification is possible with an eID method that has a substantial or high level of reliability.[40] When there is no substantial or high level of reliability, whether the means are considered sufficiently reliable according to the BFT depends on the risk of money laundering and/or terrorist financing. The BFT is of the opinion that remote identity verification can only take place for customers with low risk of money laundering and/or terrorist financing when there is no eID method with a substantial or high level of reliability.

When two-way audiovisual communication tools are used, the institution compares the received copy of the ID document with the customer and the original ID document displayed on screen. The BFT

[37] Of course, the requirements set by the Chamber of Commerce for the submission of the BO register also apply.

[38] Article 33 of the Wwft.

[39] In the eIDAS Regulation (Regulation (EU) 910/2014), three levels of reliability are defined: low, substantial and high. An eID method is sufficiently reliable when it meets the substantial or high reliability level. An institution considering accepting the use of an eID method for customer due diligence is responsible for determining whether the eID method in question is a sufficiently reliable identification tool. You can find the approved eID means in the eIDAS Dashboard (europa.eu).
Based on the Wwft, the BFT has no role in testing specific eID methods against the reliability levels defined in the eIDAS Regulation prior to their use. In the Netherlands, service providers can qualify to provide trust services through the Dutch Authority for Digital Infrastructure (Elektronische vertrouwensdiensten | Rijksinspectie Digitale Infrastructuur (RDI)). RDI is also the supervisory authority for both qualified and non-qualified providers of trust services.

[40] At the time of the publication of this Specific Guideline, no eID methods in the Netherlands have been designated with the substantial or high reliability level. However, an institution can use an eID method that has the substantial or high reliability level in another country.

recommends keeping a proper record of this conversation. This can be supplemented with a € 0.01 transfer made by the customer[41].

For customers with a medium or higher risk of money laundering and/or terrorist financing, the Wwft, in the BFT's opinion, currently does not provide options for verifying the identity using an eID method with a low reliability level or two-way audiovisual communication tools.

The BFT emphasises the importance of properly classifying the customer's risk.

The Wwft allows for the verification of the customer's identity to be carried out by third parties[42] or for an assignment to be given for the verification of the customer's identity by a third party[43]. In both cases, the institution remains responsible for ensuring the correct execution of the customer due diligence.

7.2.3 Keeping customer due diligence data up to date

A customer due diligence must not only be conducted for new customers. In some cases, a customer due diligence must also be conducted for existing customers, namely when
i) there are indications that the customer is involved in money laundering and/or terrorist financing;
ii) there is an increased risk that the customer is involved in such activities;
iii) the institution doubts the accuracy or completeness of previously obtained data;
iv) there is a higher risk of money laundering (for example, involving PEPs) and/or terrorist financing due to the country where the customer resides, is established or has its registered office.

Furthermore, an institution is obliged to take reasonable measures to keep the data collected in the context of customer due diligence up to date. Whether and how often an institution must update the data depends, in part, on the customer's risk profile (and any changes therein). The data that must be kept up to date includes data about the customer, its UBOs, representatives and its risk profile.

Wwft institutions must update the data they have collected for customer due diligence under Article 3(11) of the Wwft, at least when:

- relevant circumstances regarding the customer change;
- the institution is statutorily required to contact the customer to evaluate information about the Ultimate Beneficial Owner; or
- the institution is required to do so under Directive 2011/16/EU regarding administrative cooperation in the field of taxation.

It is not mandatory to re-verify the identity of natural persons when the validity date of the identity document shown has expired in the meantime; however, this may be important for monitoring purposes. An initial identification of a customer must always be conducted using a valid identity document.

It is important that the institution retains **all** customer due diligence data for five years after a transaction or the termination of the customer relationship. The institution must destroy any personal data it has collected under the Wwft immediately after the expiration of the five-year period, unless a statutory provision dictates otherwise.

[41] A €0.01 transfer is a method to verify the customer's identity, as the name and account number of the customer are visible. It is important that the transfer is made from a bank account in the name of the actual customer.
[42] Article 5(1)(a) of the Wwft.
[43] Article 10 of the Wwft.

7.2.4 Ultimate Beneficial Owner

7.2.4.1 Who qualifies as an UBO?

An Ultimate Beneficial Owner (UBO) is defined as any **natural person** who ultimately owns or has control over a customer, or the natural person on whose behalf a transaction or activity is being conducted.[44]

The 2018 Wwft Implementing Decree[45] provides a more detailed explanation of the definition of BO for the various legal forms. This further elaboration specifies which persons must at a minimum be considered as BOs. This can be outlined as follows:

Legal form	BO
Private limited companies and public limited companies (except listed companies and their wholly-owned subsidiaries)	• Natural person who ultimately owns or controls the legal person through: – directly or indirectly holding more than 25 per cent of the number of shares, voting rights or ownership interest (including bearer shares), or – other means, including the conditions for consolidation of financial statements referred to in Article 406 in conjunction with Article 24a, 24b and 24d of Book 2 of the Dutch Civil Code; or • Senior management (e.g. board under the articles of association[46]) – possible only if, after exhausting all possible means, no UBO has been identified or there is doubt about the identified UBO and there are no grounds for suspicion.
Churches	• Natural person who, upon the dissolution of the church, is appointed as the legal successor in the constitution of the church; or • Natural person listed as a leader in their own constitution or listed as a leader in the documents of the church organisation – possible only if, after exhausting all possible means, no UBO has been identified or there is doubt about the identified UBO and there are no grounds for suspicion.
Other legal persons (i.e. association, mutual insurance association, cooperative and foundation)	• Natural person who ultimately owns or controls the legal person through: – the direct or indirect holding of more than 25 percent of the ownership interest; – the direct or indirect ability to exercise more than 25 percent of the voting rights in decisions related to amendments to the articles of association; or – the ability to exercise effective control; or • Senior management (board under the articles of association) – only possible if, after exhausting all possible means, no UBO has been identified, or there is doubt about the identified UBO and there are no grounds for suspicion.
Partnerships	• Natural person who ultimately owns or controls the legal person through: – the direct or indirect holding of more than 25 per cent of the ownership interest in the partnership; – the direct or indirect ability to exercise more than 25 per cent of the voting rights in decisions concerning changes or execution of the agreement underlying the partnership; or – the ability to exercise effective control • Senior management (partners[47]) – only possible if, after exhausting all possible means, no UBO has been identified, or there is doubt about the identified UBO and there are no grounds for suspicion.
Trusts	• Settlor(s); • Trustee(s); • Protector(s), in so far as applicable; • Beneficiary/beneficiaries, or to the extent that the individual persons who are the beneficiaries of the trust cannot be determined, the group of persons for whose benefit the trust was primarily established or is operating • Any other natural person who exercises ultimate control over the trust

[44] The general part of the definition of 'Ultimate Beneficial Owner' is contained in Article 1 of the Wwft.
[45] Article 3 of the 2018 Wwft Implementing Decree.
[46] Senate, session year 2019-2020, 35179, C, page 13: all members of the board must be designated as BOs in such a case.
[47] With the exception of limited partners.

Source: General Guideline

This is explicitly not an exhaustive list of the possible UBOs of a customer. It is important that, once an UBO has been identified, the institution assesses whether other natural persons must also be considered as UBOs based on the remaining criteria, for example:

- by establishing a right of usufruct or a pledge on shares, where the voting rights belong to the usufructuary or pledgee, the pledgee or usufructuary may be considered the UBO of a company.
- cases where a natural person, as a shareholder, has the right to appoint or dismiss the majority of the board members of a company, regardless of the percentage of shares held.
- natural persons who, based on an agreement with the company, can exert dominant influence over the company, such as in the case of beneficial ownership.
- when voting agreements are used with multiple shareholders. These voting agreements may be relevant for customer due diligence, especially if they include arrangements on how votes are cast during shareholder meetings.
  If the key shareholders' resolutions are adopted by the same person, this may be an indication that they have effective control. Requesting, for example, shareholders' agreements can be helpful in determining the UBO.

It is the responsibility of the institution to request data that demonstrates why someone qualifies as an UBO. This may include extracts from the Commercial Register held by the Chamber of Commerce (KvK), shareholders' register, the company contract, partnership agreement, depositary receipt holders, administrative conditions of a STAK[48] and the trust deed.
Institutions may use the UBO register – after conducting their own customer due diligence – as a *tool*, but they may not solely rely on the information from the UBO register to meet their customer due diligence obligations.

7.2.4.2 Pseudo-UBO

In certain cases, all members of the senior management must be listed as UBOs, referred to as 'pseudo-UBOs'. This occurs, for example, when no UBO can be identified based on shares, voting rights or ownership, or in cases where there is doubt as to whether the identified natural persons actually have ultimate ownership or control.

However, an institution must have exhausted all possible means to identify an UBO before concluding that a pseudo-UBO exists (fallback option). In principle, an UBO must always be identified.[49] If a pseudo-UBO is identified, the measures taken and the difficulties encountered during the verification process must be documented.

The fallback option of designating senior management as UBOs applies as a (high) exception, as the UBO is typically a natural person who holds shares, voting rights or an ownership interest in a legal entity. In cases of doubt about designating someone as an UBO, the natural person who holds ownership or control takes precedence over the senior management, as otherwise, the exception would become the rule[50].

[48] STAK: Trust Office Foundation
[49] The General Guideline notes the following exception: it is not necessary under the Wwft for listed companies and their wholly-owned subsidiaries to identify the Beneficial Owners themselves. However, conditions are attached to disclosure requirements (page 30 of the General Guideline).
[50] The explanatory notes to the 2018 Wwft Implementing Decree state that members of senior management can only be considered BOs if all possible measures have been deployed by an institution to determine a customer's BOs on the aforementioned grounds (page 29). In this case, a pseudo-BO is involved.

If there are grounds for suspicion of money laundering or terrorist financing, an institution is obliged under the Wwft – when no UBO can be identified – to refuse or terminate its services, as it would not be able to fulfil the customer due diligence requirements.

7.2.4.3 Examples of Identifying UBOs

Examples of identifying BOs are included in an annex (Dutch only). These examples cover:

- private limited companies and public limited companies;
- Trust Office Foundation (STAK);
- foundations;
- associations;
- Private Foundation;
- foreign legal forms; and
- partnerships.

7.2.5 UBO register

As from 27 September 2020, companies and other legal entities are required to obtain (and maintain) information and documents about who their UBOs are. This information and documentation must be sufficient, accurate and up to date. An UBO must provide the company or other legal entity with all necessary information to comply with this requirement.

The Dutch UBO register is part of the Commercial Register maintained by the Chamber of Commerce. An institution must report to the Chamber of Commerce any discrepancies it finds between UBO information obtained from the Commercial Register and the information it holds about the UBO from other sources (the feedback obligation[51]). This obligation does not apply if an institution reports a completed or intended unusual transaction to FIU-NL.

Since the ruling by the Court of Justice of the European Union on 22 November 2022[52], it is no longer possible to request an extract from the UBO register. As a result of this ruling, a legislative proposal has been made to restrict access to the register for specifically designated parties (Amendment Act Limiting Access to UBO registers).

Transitional arrangement for new customers until 1 August 2024

Until 1 August 2024, a Wwft institution can determine whether a legal entity is registered in the UBO register based on the confirmation email from the Chamber of Commerce. This arrangement will expire on 1 August 2024.

Transitional arrangement for new customers as from 1 August 2024

As from 1 August 2024, a Wwft institution can request a certified extract from the UBO register from the customer with whom the institution is establishing a new business relationship. The customer can obtain this certified extract from the Chamber of Commerce and then provide it to the Wwft institution.

This is a transitional arrangement, and therefore a temporary measure. Once a Wwft institution is connected to the UBO register, the statutory obligation under Article 4(2) of the Wwft will apply, requiring the institution to consult the UBO register directly. It is expected that, from that point on, reporting discrepancies in UBO data to the Chamber of Commerce will also be possible again.

[51] Article 10c(1) of the Wwft.
[52] See also: ECLI:EU:C:2022:912.

The BFT advises institutions to follow developments in this area and, when it is again possible to consult the UBO register, comply with the feedback obligation where necessary.

Feedback obligation for certified extracts as from 1 October 2024

If a Wwft institution is connected to the UBO register and notices discrepancies between the data in the UBO register and other information sources, the Wwft institution is obliged to submit a feedback notification to the Chamber of Commerce. This is known as the feedback obligation.

As from 1 October 2024, this feedback obligation will also apply if a Wwft institution receives a certified extract from a customer and notices discrepancies. Since the process of requesting a certified extract from the customer is new for Wwft institutions, a bridging period has been provided until 1 October 2024. During this time, the feedback obligation will not apply.

Reporting discrepancies until 1 October 2024 is allowed but not mandatory. The obligation to report these discrepancies to the Chamber of Commerce based on a certified extract received from a customer will apply once a Wwft institution is again able to consult the UBO register. After all, from that moment onwards, the Wwft institution will be able to report back any discrepancies detected based on the self-obtained data to the Chamber of Commerce.

7.3 Simplified customer due diligence

An institution must – based on a risk assessment – determine whether simplified customer due diligence can be applied before entering into a business relationship or performing a one-off transaction. The customer due diligence can under no circumstances be omitted. The institution conducts standard due diligence, but with less depth. Identifying the customer and verifying their identity is therefore necessary. However, the institution may use sources of lower reliability or a lower number of sources for verifying identity.

According to Article 6 of the Wwft, an institution must consider the risk factors outlined in Annex II to the Fourth Directive to assess whether there is a lower risk of money laundering and terrorist financing, justifying simplified customer due diligence. This annex includes the following (non-exhaustive) list of factors and types of evidence of potentially lower risk:

1. *Customer-related risk factors:*

- listed companies[53] subject to disclosure requirements (under stock exchange rules or statutory or enforceable means), which include provisions to ensure adequate transparency regarding the Ultimate Beneficial Owners[54];
- governments or public companies;
- customers who are residents of geographical areas with a lower risk (as mentioned below in point 3).

2. *Product, service, transaction or delivery channel-related risk factors:*

- life insurance policies with low premiums;
- pension insurance contracts that do not include a surrender clause and cannot be used as collateral;
- a pension scheme, pension fund or similar system that provides pensions to employees, where contributions are withheld from wages and the system's rules prevent participants from transferring their rights under the system;
- financial products or services that suitably offer certain and limited services for specific types of customers, in order to increase access for financial inclusion purposes;

[53] This also applies to wholly-owned subsidiary companies of listed companies.

[54] The List of Recognised Exchanges on the website of the Dutch Banking Association (NVB) can be helpful in this regard.

- products where the money laundering risk and terrorist financing risk are mitigated by other factors, such as spending limits or ownership transparency (e.g. certain types of electronic money).

In addition to Annex II to the Fourth Directive, a lower risk of money laundering may apply to the following services:

- simple income tax returns (without taxable profits from business activities, without taxable results from other activities, without substantial interest and without income from savings and investments)[55];
- gift tax and inheritance tax returns under the Inheritance Tax Act 1956[55].

3. Geographical risk factors

Registration, establishment or country of residence in:

- Member States;
- third countries with effective systems to combat money laundering and terrorist financing;
- third countries that, according to credible sources, have a low level of corruption or other criminal activity;
- third countries that, according to credible sources – such as mutual evaluations, detailed evaluation reports or published follow-up reports – have anti-money laundering and terrorist financing regulations that meet the revised FATF recommendations and effectively implement these regulations.

7.4 Enhanced customer due diligence

An institution must – based on a risk assessment – determine whether enhanced customer due diligence is necessary before entering into a business relationship or performing a one-off transaction. The monitoring obligation may also require enhanced customer due diligence if, for example, there is a change in the customer's risk profile during the customer relationship. Article 8 of the Wwft refers to Annex III of the Fourth Directive for enhanced customer due diligence.

The Wwft prescribes enhanced customer due diligence in the following (relevant) situations:

- a higher risk of money laundering or terrorist financing;
- a customer who is resident or established, or has its registered office in a third high-risk country[56];
- complex and unusual large transactions or unusual transaction patterns with no clear economic or lawful purpose; and
- a PEP as a customer, or a customer whose UBO is a PEP.

The General Guideline provides the following examples of activities in the context of enhanced customer due diligence:

- requesting a certificate of conduct from the legal entity; the customer's codes of conduct and/or whistleblowers' schemes;
- requesting information about internal procedures, internal control measures and compliance with these measures;
- further investigating the powers and functions of the board of directors and authorised representatives (in relation to segregation of duties and conflicts of interest);
- investigating the customer's customers and/or intermediaries;
- presence of internal fraud risks and fraud prevention measures;
- investigating the origin and destination of funds, including requesting bank statements.

[55] These activities were subject to a customer due diligence exemption until 25 July 2018 (Article 2 of the Wwft Implementing Regulations until 25 July 2018). This exemption was lifted on that date.

[56] See also '3. Geographical risk factors' in this section.

7.4.1 Higher Wwft risk

Depending on the specific facts and circumstances and the professional judgment of the institution, it must be assessed whether there is an increased risk. In many cases, an increased risk will only arise if a combination of points of consideration occurs, which must be viewed in interrelation.

To provide institutions with practical guidance, an integrated list of risk factors has been created. The BFT would like to emphasise that if a branch of industry is included as an example of a point of consideration, this does not automatically mean that there is a higher risk. The institution must assess this on a case-by-case basis. The BFT recommends that institutions document their considerations in the file.

1. Customer-related risk factors

Below are some non-exhaustive points of consideration that may assist the institution in assessing customer-related risk factors.

a. *Based on activities*:

1. Customers with significant amounts of **cash** available.
   Examples: hospitality businesses, currency exchange offices, (high-value) traders, jewellers, souvenir shops;
2. Businesses that have been shown in practice to be potentially vulnerable to official or unofficial **corruption** – with or without procurement-related activity.
   Examples: property sector, construction/infrastructure, government, semi-public sector, pharmaceutical sector, extraction and trade in raw materials, energy and telecom sectors[57];
3. Businesses where the price of goods and/or services **cannot objectively** be determined.
   Examples: art and antiques, football agents, agent payments, commission payments;
4. Customers who may be involved in the **evasion of tax regulations**.
   Examples: VAT carousel fraud, failure to file tax returns, large supplementary returns without plausible reasons[58];
5. Businesses that have been found in practice to potentially be used for **underground banking**.
   Examples: phone shops, money (exchange) offices, travel agencies;
6. Businesses dealing in **drug-related** products.
   Examples: coffee shops, grow shops;
7. Customers against whom action has been taken under **sanction**s legislation;
8. Customers involved in or assisting with circumventing **sanction**s legislation;
9. Customers dealing in or paying with **virtual currencies**;
10. Businesses that have been shown in practice to be potentially vulnerable to **undermining** activities.
    Undermining refers to the blending of the underworld with the legitimate society and manifests in various forms. This could include providing meeting places for criminal activities, offering support services and providing auxiliary services[59].

b. *Based on the organisational and financing structure:*

1. Customers who are part of an **opaque** or **complex** ownership or control structure.
   Examples: offshore companies; use of nominees, bearer shares, 'shell companies' or 'dormant companies', use of postal addresses;
2. Customers who own legal entities or legal constructs that serve as vehicles for holding personal assets.
   Examples: certain trusts or foundations in which assets are held;

[57] See also: NBA Practice Note 1137 - Corruption: procedures for auditors

[58] Large supplementary returns may have been caused if the tax authorities have been used as the customer's 'funder'. This could raise a suspicion of VAT fraud.

[59] The Kennisplatform Ondermijning contains information about undermining and its approach (https://www.kennisplatformondermijning.nl/).

3. Customers who possess assets with **unclear origins**.
   Examples: loan-back structures, crowdfunding, fundraising activities (whether online or in person), financing outside the regular sector, use of virtual currencies;
4. Customers where ***cash compensation*** may be involved.[60]
   Example: companies in labour-intensive sectors such as construction and parcel delivery outsource work to contractors (or subcontractors) and pay them via bank transfer. However, these subcontractors rarely or never make bank transfers for wages, and employees are paid in cash. FIU-NL has indications that the cash used for this often has a criminal origin. This cash, purchased from criminals, is compensated by subcontractors through bank (invoice) payments.
5. Spending of funds by customers may indicate **terrorist financing**.

c. Based on the service requested:

1. Customers involving (one-off) complex urgent services for no apparent reason;
2. The service the customer requests does not fit the institution's usual pattern;
3. The usual reasons for engaging the institution seem to be absent.

d. Other points of consideration:

1. Customers who provide false or incomplete information, or where there is doubt about the accuracy or completeness of the information provided;
2. Customers with an unclear or changing business address without an explanation being provided;
3. Customers whose business activities are unclear or who use intermediaries whose role is unclear;
4. Customers who are residents of geographical areas with higher risks (see Geographical risk factors).
5. A customer who is a national of a third country applying for residence rights or citizenship in the Member State in exchange for capital transfers, the purchase of immovable property, government bonds or investments in companies in that Member State.

2. Product, service, transaction or delivery channel-related risk factors

Below are some non-exhaustive points of consideration that may assist the institution in assessing product, service, transaction and delivery channel-related risk factors.

a. Product and service-related risk factors

1. Fraud investigations;
2. Products or transactions that promote anonymity.
   Example: customers using virtual currencies (such as Bitcoins or other cryptocurrencies);
3. An employee of an institution holding an organisational position with a customer;
4. Services related to the assignment or settlement of receivables whose value is difficult to determine;
5. Use of unnecessarily complex corporate structures;
6. Advising on cash companies[61];
7. Services involving the creation of international structures to conceal the UBO;
8. Advising on back-to-back loans and loan-back constructs;
9. Transfer pricing: advising on transactions between affiliated parties.
   Example: transactions that are not at arm's length, where questions may be raised about the value of the performed deliverables or counter-deliverables.

[60] FIU-NL explained the money laundering cash compensation methodology in its 2023 Annual Report (Dutch only).
[61] Cash companies are companies that have ceased operations and have a high cash or bank balance as a result of the sale of their assets. By creating tax liabilities in the company, the material tax liability falls away, releasing the reserved liquid assets (ECLI:NL:GHAMS:2007:BB 2447).

b. Transaction-related risk factors

1. Businesses that can be used for Trade-Based Money Laundering (TBML).
   Examples: payments to a supplier by non-affiliated third parties; misrepresentation of prices, carousel transactions, goods that do not fit within regular trade, double invoicing of goods.
2. Mergers or acquisitions where the buyer uses unconventional financing structures.
   Examples: financing from an unconventional country, use of unusual terms.
3. Use of companies whose:
   - assets do not truly exist or are hidden;
   - accounting records are missing;
   - publication requirements are not met; or
   - no business activities are carried out;
4. Share transactions where the value of the shares is difficult to determine;
5. Transactions involving financing outside the regular financial sector.
   Examples: (cash) loans (from family) from abroad, underground banking;
6. Drafting private loan agreements or loan notes where the source of financing is unclear;
7. (Tax or other) authorities requesting further information about the customer or UBO;
8. Transactions related to crude oil, weapons, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious significance or of great scientific value, as well as ivory and protected species.

c. Delivery channel-related risk factors

1. Business relationships or transactions conducted remotely from the customer, without certain guarantees, such as electronic identification means or relevant trust services as defined in Regulation (EU) No. 910/2014, or any other identification process that is secure, conducted remotely or electronically, and regulated, recognised, approved or accepted by the relevant national authorities.

3. Geographical risk factors

The EU regularly publishes a list of high-risk countries.[62]
Under Article 8(1)(b) of the Wwft, enhanced customer due diligence must be conducted when the customer is resident, established or has its registered office in one of these countries.

For the countries listed below, enhanced customer due diligence is not mandatory under Article 8 of the Wwft. An institution must include the geographical risk as part of the risk assessment.

- The **FATF** assesses multiple times a year which countries have a high risk of abuse in the context of money laundering and terrorist financing (high-risk jurisdictions). The FATF also publishes a list of countries under increased monitoring. Consult the FATF website for the current status of countries included.
- **Transparency International** annually publishes the Corruption Perception Index. The list is an indicator of how the public sector of different countries is perceived in terms of freedom from corruption.
- In investigations into **property fraud**, the following countries or states, in addition to the EU high-risk countries list, have been identified as having a higher risk of money laundering: Andorra, Anguilla, British Virgin Islands, Curacao, Delaware, Guernsey, Hong Kong, Jersey, Liechtenstein, Luxembourg and Switzerland. Depending on the type of transaction being conducted and the customer's overall risk profile, there may be an increased risk of money laundering or terrorist financing.
- **Investigations by the BFT** have shown that, in addition to the EU high-risk countries list, Cyprus and Malta may be considered higher-risk countries. It should be noted that it is not the country itself that

[62] In principle, the EU follows the FATF list, but there are differences between the two lists. For example, no country from the internal market is included on the EU list.

automatically presents a higher risk, but rather the combination of the country with the types of transactions conducted (property transactions and/or international (tax) structures with foreign companies or trusts).

Regarding geographical risks, further consideration could be given to:

- countries subject to sanctions, embargoes or similar measures issued, for example, by the European Union (EU) or the United Nations (UN);
- countries that provide funding or support for terrorist activities or in whose territory organisations designated as terrorist are active (e.g. Al Nusra, Al Shabaab, Islamic State (IS), Al Qaida). Examples of countries include Iraq, Iran, Yemen, Kuwait, Qatar, Saudi Arabia and Syria;
- tax havens, whether current or former, or countries with which information exchange is difficult[63];
- countries where offshore companies are often established (e.g., British Virgin Islands, Belize).

7.4.2 Measures in case of high-risk countries

An institution must carry out enhanced due diligence measures when transactions and/or business relationships are related to countries with a higher risk of money laundering or terrorist financing (high-risk countries[64])[65]. According to the Wwft, the following enhanced due diligence measures are required[66]:

1. collecting additional information about customers and UBOs;
2. collecting additional information regarding the purpose and nature of the business relationship;
3. collecting information about the origin of the funds used in the business relationship or transaction and the source of assets of customers and UBOs;
4. collecting information about the background of and reasons for the proposed or completed transactions of customers;
5. obtaining approval from senior management for entering into or continuing the business relationship;
6. performing enhanced monitoring of the business relationship with and transactions of customers. This includes increasing the number of checks and the frequency of updates of customer and UBO information, as well as selecting transaction patterns that need further investigation.

7.4.3 Measures in case of complex and unusually large transactions and unusual transaction patterns

An institution must take reasonable measures to investigate the background and purpose of:

- complex transactions;
- unusually large transactions;
- transactions with an unusual pattern;
- transactions without a clear economic or lawful purpose.

If any of the above apply, the entire business relationship must be subjected to enhanced monitoring.

For the assessment of an unusually large transaction or unusual transaction pattern, the institution must take into account the customer's (risk) profile. This (risk) profile is established prior to the customer due diligence. The institution must determine whether a transaction fits within this (risk) profile.

[63] See also: *Regeling laagbelastende staten en niet-coöperatieve rechtsgebieden voor belastingdoeleinden* (Regulation on low-tax states and non-cooperative jurisdictions for tax purposes) and the explanatory notes to the regulation (Dutch only).
[64] High-risk countries according to the European Commission.
[65] The BFT notes that, based on (other) geographical risks, enhanced due diligence measures may also need to be carried out.
[66] General Guideline, page 41.

If this is not the case, there is a basis for taking enhanced measures and more intensive monitoring. If necessary, the institution will report the transaction as unusual.

7.4.4 Measures in case of PEPs[67]

PEPs refer to individuals who hold or have held a prominent public function, as well as their immediate family members or close associates.

An institution must make reasonable efforts to identify a PEP. Whether an institution has made reasonable efforts is dependent on whether it has procedures in place for this purpose. The method of identifying a PEP is not prescribed by regulation. In practice, the BFT observes the use of:

- PEP declaration or PEP questionnaire;
- internal research; and/or
- consulting databases (whether commercial or public).

A PEP is at least[68]:

1. head of state, government leader, minister, deputy minister or state secretary;
2. member of parliament or a similar legislative body;
3. member of the governing body of a political party;
4. member of a court of last resort, constitutional court or another high judicial authority whose rulings are not subject to appeal except in exceptional circumstances;
5. member of an audit office or the board of a central bank;
6. ambassador, chargé d'affaires or senior military officer;
7. member of the governing, supervisory or management body of a state-owned enterprise;
8. director, deputy director, member of the board of directors or equivalent role at an international organisation.

In addition, the Ministries of Finance and Justice and Security have compiled a list detailing the positions that qualify as politically prominent in the Netherlands. This list is included in the General Guideline. At the European level, several countries have also created a (non-exhaustive) list of politically prominent functions.[69]

Mid-level or lower-ranking officials do not qualify as PEPs, which includes local or regional politicians. However, even if someone is not a PEP, a higher risk may still be present based on their position (due to potential for misuse).

When a person is identified as a PEP, the following requirements must be met according to Article 8 of the Wwft:

- prior to establishing or continuing the business relationship, consent must be obtained from a senior management member of the institution;
- the source of wealth and funds involved in the transaction or business relationship must be established;
- the institution must continuously conduct enhanced monitoring on this business relationship;
- the measures must also apply to the family members or close associates of PEPs; and
- the collected data must be kept up to date.

[67] PEP stands for Politically Exposed Person.
[68] See also Article 2(1) of the 2018 Wwft Implementing Decree
[69] Prominent public positions at the national level, at the level of international organisations and at the level of Union institutions and bodies.

If, during the business relationship, a customer or BO becomes or is identified as a PEP, the requirements outlined above must be immediately and promptly fulfilled.

7.4.4.1 Family members and close associates of PEPs

The Wwft institution must also apply enhanced customer due diligence measures to certain family members and close associates of PEPs.

Family members of a PEP

- The spouse or a person considered equivalent to the spouse of a PEP (e.g. a registered partner);
- A child of a PEP (by birth, acknowledgment, judicial determination of parentage or adoption), the spouse of that child or a person considered equivalent to the spouse of that child;
- The parent of a PEP.

Close associates of a PEP

- A natural person known to jointly hold UBO status with a PEP in a legal entity or legal construct, or who has other close business relationships with a PEP;
- A natural person who is the sole UBO of a legal entity or legal construct known to have been set up for the actual benefit of a PEP.

7.5 Customer due diligence by third parties

An institution can have the customer due diligence performed partially by a third party (outsourcing of the customer due diligence)[70]. It is also permitted to adopt the customer due diligence conducted by another designated Wwft institution (introductory customer due diligence)[71]. However, the institution itself remains ultimately responsible for compliance with the Wwft.

For example, an institution may use a CDD[72] service provider. If this outsourcing is of a structural nature, the institution must formalise the contract to that effect in writing.
Before contracting an external party, it is important to assess whether they align with the institution's customer portfolio. For instance, if an institution has an international customer base, it is essential not only to consult the Dutch Commercial Register but also registers in countries where the customers are active. The institution must also verify afterwards that the customer due diligence performed meets the Wwft obligations. If necessary, the institution must carry out additional work.
An institution must be aware that CDD systems can be input-sensitive: an input error may lead to an incorrect output from the system, which could lead the institution to draw incorrect conclusions.

Ongoing monitoring of the business relationship and the transactions performed during the course of that relationship (monitoring obligation) **cannot** be outsourced.

8. Monitoring obligation

8.1 General

The Wwft requires an institution to conduct ongoing monitoring of the business relationship and the transactions carried out during its duration.[73]

[70] Article 10(1) of the Wwft.
[71] Article 5(1)(a) of the Wwft.
[72] CDD: customer due diligence.
[73] Article 3(2)(d) of the Wwft.

In this manner, an institution ensures that the relationship and transactions align with the knowledge it has of the customer and its **risk profile**. An institution must establish a separate risk profile for each customer at the start of the service provision.

An institution can only recognise unusual transactions if it has a good understanding of its customer. If certain transactions indicate that the customer deviates from this profile, it must be determined what risks this poses. As stated in Chapter 7, the depth of customer due diligence also depends on the customer's risk profile.

According to the Wwft, an institution must, if necessary, investigate the source of the funds used in the business relationship or transaction. This also falls under the monitoring obligation.

If, as a result of monitoring, the customer's risk profile changes, the institution may (still) have to perform an enhanced customer due diligence (Section 7.4).

8.2 Monitoring risk profile and transactions

While carrying out its activities, an institution may find it necessary to conduct further investigation into transactions. This could involve asking additional questions and obtaining further clarification. It is important for the fulfilment of the monitoring obligation that the answers are concrete, somewhat verifiable and not deemed completely implausible from the outset. Generally, only a verbal explanation from the customer is not sufficient.

Below are some non-exhaustive points of consideration that can assist an institution in determining when additional actions must be taken. The customer is involved in:

- changes in ownership and control relationships;
- changes in the board, but the 'old' board members continue to de facto hold power;
- changes or expansion of activities;
- (significant) margin changes compared to industry data or previous periods;
- income that is not aligned with expenses, raising the question of how the customer sustains itself;
- a non-reconciling flow of funds or assets;
- frequent general journal entries or correction entries in the accounts;
- special, one-off or large/complex transactions;
- (occasional) transactions with unknown parties;
- non-business or non-market-compliant terms in contracts (e.g. loan agreements, lease agreements, purchase agreements, sales agreements);
- the absence of contracts;
- discrepancies between the financial statements or tax returns and underlying documents;
- a negative cash balance;
- specifications that do not match underlying documents or the financial statements/tax return;
- frequent or large supplementary returns;
- legal proceedings.

8.3 Source of funds

The monitoring obligation is based on the premise that, if necessary, the institution investigates the source of funds used in a business relationship or transaction. The investigation is risk-based.

The institution must record statements and/or objective and independent documents about the source of the funds as evidence in the customer file. This may include a statement from the customer, supplemented with documents such as income tax returns, gift or inheritance tax returns, bank

statements, loan agreements, as well as annual reports and accounts. If necessary, the institution must ask additional questions.

9. Obligation to report unusual transactions

9.1 Reporting (completed and intended) unusual transactions

9.1.1 General

As mentioned in Chapter 2, money laundering generally refers to mixing illegal money flows with legal ones in order to give the illegal money flows a legitimate status. Terrorist financing refers to the use of funds to facilitate terrorist activities.

For an institution, two indicators are important in determining whether a transaction is unusual: the objective indicator and the subjective indicator[74].

The BFT wishes to emphasise that the 'unusual' in the term unusual transaction refers exclusively to possible money laundering – including the underlying offences of money laundering – and/or terrorist financing. A transaction that is common for a customer or within the industry in which they operate is not automatically considered usual.

The obligation to report applies to both completed and intended (but not yet completed) transactions.

As outlined in the General Guideline, Wwft institutions and the individuals working for them are bound by a general confidentiality obligation regarding reports made by the Wwft institution to FIU-NL under Article 16 of the Wwft and with respect to further data and information provided by the Wwft institution to FIU-NL under Article 17 of the Wwft.

9.1.2 Objective indicator

The objective indicator under the Wwft is defined for institutions falling under Article 1a(4)(a) and (b) of the Wwft as a transaction amounting to € 10,000 or more, paid in cash or similar payment methods, either directly to or via the institution.

This means that these institutions are *always* required to report an unusual transaction if the transaction meets the objective indicator. This can be a single payment or a series of payments (whether full or partial) from a single customer that together exceed € 10,000 (smurfing).

In addition, FIU-NL's website includes the following objective indicator: *"It stands to reason that transactions reported to the police or Public Prosecution Service in connection with money laundering or terrorist financing must also be reported to the Financial Intelligence Unit; after all, there is a presumption that these transactions may be related to money laundering or terrorist financing."*

Third high-risk countries

From 25 July 2018 to 18 October 2019, the Wwft included an objective indicator for mandatory reporting of unusual transactions involving third high-risk countries.

[74] Article 15(1) of the Wwft in conjunction with Article 4 of the 2018 Wwft Implementing Decree and the indicator list annexed to this Implementing Decree.

The removal of this objective indicator does not mean that an institution no longer has to report transactions related to third high-risk countries. Based on the subjective indicator, any transaction that raises suspicion of being related to money laundering or terrorist financing must still be reported.

9.1.3 Subjective indicator

The subjective indicator is defined as a transaction where the institution has reason to suspect that it **may** be related to money laundering or terrorist financing.
This means that an institution must consider, based on the knowledge it has gained in the course of its profession and its understanding of the customer, whether a transaction could be unusual.

The reporting obligation is low-threshold. The obligation to report an unusual transaction does not arise only when there are concrete indications that the transaction is related to money laundering or terrorist financing. Article 16 of the Wwft has a broader scope: **any** (completed or intended) unusual transaction must be reported.

Annex 1 to the Specific Guideline provides examples that may be helpful in determining whether, based on the subjective indicator, an unusual transaction must be reported.

If a case is described in Annex 1, the professional must be alert. If one or more of the listed examples apply, this may be an important indication that the transaction is unusual[75]. The examples outlined can be considered potentially unusual if **no** acceptable explanation can be provided for the institution.

The institution must therefore conduct further investigation, ask additional questions, obtain further substantiation, document the results of this investigation and, if necessary, file a report of an unusual transaction. The professional evaluates, based on known facts and circumstances, whether there is reason to suspect that the transaction **may** be related to money laundering and/or terrorist financing. The BFT emphasises that the examples are non-exhaustive.

This does not preclude other ways to apply the subjective indicator, such as well-known money laundering typologies and facts of common knowledge used in criminal law.[76]

9.1.4 Reporting in case of failed customer due diligence or termination of the relationship

If customer due diligence cannot be carried out with sufficient results **and** there are indications that the customer is involved in money laundering or terrorist financing, an unusual transaction is considered to have occurred under Article 16(4) of the Wwft.

If an institution terminates a business relationship **and** there are indications of money laundering or terrorist financing, a report must be made regarding a (completed or intended) unusual transaction. The institution must then state the reasons for terminating the business relationship and provide any indications of money laundering or terrorist financing. The decision to terminate the business relationship may relate to both the monitoring obligation and the customer due diligence. The latter applies when the exception was used to start the services before completing the customer due diligence (Article 4(5) of the Wwft).

9.2 Reporting obligation for interdisciplinary collaborating institutions

It is possible that various disciplines collaborate within a legal entity. Examples of collaborations include:

[75] The fact that a particular example is not included in Annex 1 cannot be taken to mean that therefore the transaction is not or cannot be unusual.
[76] Examples of money laundering typologies can be found on the FIU-NL website and the AMLC website.

- administrator and tax consultant;
- accountant and tax consultant; or
- tax consultant and civil-law notary.

In practice, there is sometimes uncertainty regarding which reporting code an institution should use for a Wwft report. This arises because – based on the Wwft – these legal entities must register separately with FIU-NL for each professional activity.

What must be reported under which reporting code?
It is not the intention for a legal entity to make double reports, i.e., reports with the same content under two different reporting codes. One report is sufficient. If there is doubt about the correct reporting code, it is more important to file the report than to use the correct reporting code.

- If one of the disciplines carries out work for a customer, the report must be filed under the reporting code of that discipline.
- When multiple disciplines are involved in the work, the following applies:
  - initially, the primary activity of the assignment determines under which reporting code a legal entity must report an unusual transaction.
  - the following exception applies: if the unusual transaction is observed in the performance of work that does not constitute the primary activity, the nature of the work determines under which reporting code the legal entity must file the report.

9.3 Reporting obligation when the customer is a Wwft institution

The reporting obligation of an institution is not affected by the reporting obligation of another institution involved in a transaction. The rationale behind this is that multiple, different reports about the same transaction can improve the quality of the FIU-NL database. Additionally, it provides more assurance that the transaction is actually reported.

If the customer of an institution is itself also a institution obliged to notify under the Wwft, the institution must determine whether the customer has already reported the unusual transaction(s) in good faith, based on their own reporting obligation.[77] If this has been done, the BFT recommends (preferably) keeping a copy of the report(s) and the acknowledgment of receipt in your file.

If the customer has not reported, the institution must inform the customer, in general terms, about the existence of the reporting obligation. If the institution has indications that the customer is (deliberately) not complying with its reporting obligation, the institution itself must report the customer. After all, deliberate failure to report may be a subjective indicator.

The BFT does not consider it necessary for an institution to report again to the FIU-NL – without any additions – if the customer has made a report on the basis of its reporting obligation.
However, if the institution itself observes something that has not been included in the customer's reported transaction, it is reasonable for the institution to file its own report of an unusual transaction.[78].

9.4 Record keeping of report data

An institution must retain the following for five years after the report has been made:

- data necessary to later reconstruct the transaction;

[77] See ECLI:NL:RBAMS:2024:1750: the car company in question had reported to FIU-NL, but the actual buyers remained out of sight because strawman constructs were used'.
[78] In some cases, a trader may also have participated (passively) in transactions, for example by accepting large denominations. Other risk factors include: i) someone other than the buyer deposits or brings the money; and ii) the use of foreign companies with different addresses/descriptions.

- a copy of the report and the information provided with it; and
- acknowledgment of receipt from FIU-NL.

The institution must destroy any personal data it has collected under the Wwft immediately after the expiration of the five-year period, unless a statutory provision dictates otherwise.

9.5 Provision of information to FIU-NL

Article 16 of the Wwft describes the data that an institution must provide, namely:

a. the identity of the customer, the identity of the Ultimate Beneficial Owners and, to the extent possible, the identity of the person for whose benefit the transaction is carried out;
b. the type and number of the customer's identity document and, as far as possible, those of the other persons mentioned in point (a);
c. the nature, date and place of the transaction;
d. the amount and destination, as well as the origin, of the funds, securities, precious metals or other valuables involved in the transaction;
e. the circumstances under which the transaction is considered unusual;
f. a description of the relevant items of high value in case of a transaction above € 10,000;
g. additional data that may be designated by general administrative order.

It is important for FIU-NL that what is described under point (e) is detailed and substantiated in the transaction description of the reporting form (i.e. the link to money laundering, underlying money laundering offences and/or terrorist financing).

FIU-NL may request further information (data or intelligence) regarding reports of unusual transactions[79]. This can be requested from the reporting institution or another institution, i.e. a gatekeeper other than the gatekeeper who made the report. Responses to inquiries from FIU-NL must be provided immediately.

FIU-NL has provided an animation explaining the reporting process.

9.6 Immunity

When an institution in good faith and properly reports an unusual transaction in accordance with Article 16 of the Wwft or provides information pursuant to Article 17 of the Wwft, it receives civil non-liability and criminal immunity[80].

This criminal immunity pertains to the risk that the institution faces – if it is involved in an (unusual) transaction – of being considered a co-perpetrator or accessory in the event that the transaction is indeed connected to money laundering and/or terrorist financing. By reporting the transaction, the reporter remains exempt from potential criminal investigation related to the transaction.

The civil non-liability does not apply if, considering all the facts and circumstances, it could reasonably be said that the transaction should not have been reported.

10. Sanctions legislation

As outlined in the Ministry of Finance's financial sanctions guideline (Dutch only), non-financial businesses such as accountants, tax consultants and administrative offices must comply with the Sanctions Act.

[79] Article 17 of the Wwft.
[80] Of course, this non-liability and immunity do not apply if the institution itself is guilty or jointly guilty of money laundering or terrorist financing.

It is expected that in 2025, the BFT will be appointed as the supervisory authority for the International Sanctions Act (*Wet internationale sanctiemaatregelen*). A specific guide for this Act will follow.

11. Other

11.1 Whistleblowers and reporting centre

An institution must have adequate, appropriate provisions in place that allow employees or individuals in similar positions to anonymously report a violation of the Wwft.[81]

Additionally, individuals working for an institution must not be disadvantaged when they report internally or report to FIU-NL in good faith and properly. This also applies when the individual in question provides additional information to FIU-NL.

Employees who are disadvantaged by their institution – because they have reported a violation of the Wwft through their institution's whistleblowers' scheme – may file a complaint with the BFT. The same applies to employees who are disadvantaged because they have contributed to a report of an unusual transaction.

Furthermore, a report of wrongdoing at an institution under BFT supervision can be made via the same form.

11.2 Certificate of good conduct

The anti-money laundering directive requires measures to be taken to prevent (convicted) criminals or their accessories from holding leadership roles or being UBOs of certain Wwft institutions. This also applies to the institutions governed by this Specific Guideline.

At the request of the BFT, institutions or their policymakers must be able to provide a certificate of good conduct.

12. Enforcement

When insufficient compliance with statutory provisions and violations thereof are detected, the BFT can issue mandatory instructions to follow a certain course of action regarding the development of procedures, controls and training. Administrative or disciplinary measures may also be imposed. The BFT has the authority to impose administrative penalties and orders subject to a penalty. The BFT's fining policy (Dutch only) is published on its website.

In serious cases, the BFT may file a report with the public prosecutor, who can then initiate a criminal investigation. Non-compliance with the Wwft qualifies as an economic offence, for which, if committed intentionally, the sentence can be up to two years of imprisonment, a community punishment order or a fourth-category penalty (€ 25,750[82]). Additional penalties may also be imposed, including the complete or partial suspension of the convicted person's business, through which the economic offence was committed, for a period of up to one year.

The Wwft includes an obligation for the BFT to publish administrative sanctions on its website. This obligation relates to penalties, instructions and orders subject to a penalty. Publication may be

[81] Article 20a of the Wwft.
[82] Until 1 January 2024, this was €20,500.

anonymised or delayed only under certain circumstances. The aim is to inform and warn the market. The BFT is also authorised under the Wwft to publish a warning or statement, including the violation and the name of the offender.

13. Annexes

1. Wwft examples related to the subjective indicator
2. 2023 10-step Wwft plan (Dutch only)
3. Changes to the Wwft since 24 October 2018 (Dutch only)

Utrecht, 24 October 2024

BFT

autoriteit voor
financieel-juridisch
toezicht

Maliebaan 79 • 3581 CG Utrecht
PO Box 14052 • 3508 SC Utrecht

T +31 (0)30 251 69 84
E bft.post@bureauft.nl
W www.bureauft.nl