Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act

December 2020 version

DeNederlandscheBank

EUROSYSTEEM

Some parts of this information are no longer current and will be amended.
Please see Sanctions screening (dnb.nl).

2 This Guideline applies to institutions that are subject to DNB supervision and complements the "General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wwft*)" of the Ministry of Finance and the Ministry of Justice and Security,[1] and the "Guidance Financial Sanctions Regulation" of the Ministry of Finance.[2] The guidance documents clarify the various obligations arising from the Wwft and the Sw and provide tools for the implementation of these obligations. The other Wwft supervisory authorities also provide guidance for the institutions falling under their supervision.[3]

This Guideline is neither a legally binding document nor a DNB policy rule as referred to in Section 1:3(4) of the General Administrative Law Act (*Algemene wet bestuursrecht*) and does not have or aim to have any legal effect. This Guideline does not replace legislation and regulations, policy rules or supervisory regulations in this area. The examples in this Guideline are not exhaustive and cannot be deemed sufficient for compliance with the legal requirements in all cases. DNB intends this Guideline to serve as an aid for the explanation and application of the legal obligations.

1 Available for consultation at: https://www.rijksoverheid.nl/documenten/richtlijnen/2020/07/21/algemene-leidraad-wet-ter-voorkoming-van-witwassen-en-financieren-van-terrorisme-wwft (available in Dutch only).
2 Available for consultation at: https://www.rijksoverheid.nl/documenten/rapporten/2020/08/12/leidraad-financiele-sanctieregelgeving (available in Dutch only).
3 AFM, Tax Administration/Wwft Supervision Agency, Financial Supervision Agency, Gambling Authorities and the presidents of the Netherlands Bar.

Contents

1 Introduction 5

2 Organisation of operational management 8
2.1 Ethical operational management 8
2.2 Training and awareness 10
2.3 Ethical business culture 11
2.4 Internal whistleblower scheme and integrity reporting desk 11
2.5 Know your customer (KYC) / Customer due diligence (CDD) 12
2.6 Sanctions regulations 12
2.7 Foreign branches and subsidiaries of Dutch institutions 13

3 Risk-based thinking: the systematic integrity risk analysis 14
3.1 Organisation of integrity policy 14
3.2 Design of systematic integrity risk analysis (SIRA) 14
3.3 Risk factors 16
3.4 Classification of customers into risk categories 19
3.5 Customers and products with a heightened integrity risk 22
3.6 Unacceptable risks 23

4 Customer due diligence 25
4.1 Regulatory framework 25
4.2 Identification and verification 26
4.3 Entering into a business relationship 31
4.4 Not entering into or terminating the business relationship 33
4.5 Ultimate beneficial owner (UBO) 35
4.6 Purpose and nature of business relationship 39
4.7 Source of funds 40
4.8 Simplified customer due diligence, low-risk factors and exceptions to the customer due diligence 40
4.9 Enhanced customer due diligence and high-risk factors 43
4.10 Outsourcing 52

5 Transaction monitoring and reporting of unusual transactions 53
5.1 General information 53
5.2 Recognising patterns and transactions 55
5.3 Focus on high-risk jurisdictions 56
5.4 Assessment of transactions, measures and reporting 56
5.5 Obligation to report unusual transactions 57
5.6 FIU reporting procedure 60
5.7 Indemnification 61
5.8 Confidentiality under the Wwft 61
5.9 Legal claims and confidentiality under the Wwft 62

6 The Regulation on information accompanying transfers of funds (Wire Transfer Regulation 2) 63
6.1 General information 63
6.2 Background to WTR2 63
6.3 Scope of application 63
6.4 Obligations of payment service providers and intermediary payment service providers 63
6.5 Detecting and assessing incomplete information 64
6.6 EBA Guidelines 64
6.7 FIU notifications 64
6.8 Integrity supervision under the Wwft 64

7 Sanctions regulations 65
7.1 General information 65
7.2 Administrative organisation and internal control (AO/IC) 66
7.3 The 'relationship' concept 67
7.4 Transaction monitoring 68
7.5 Reporting to DNB 69
7.6 Hit reports, FIU reports and deadlines 70

8 Record-keeping, data retention obligation and the General Data Protection Regulation (GDPR) 72

1 Introduction

In addition to solidity, integrity is a prerequisite for a sound financial system. De Nederlandsche Bank (DNB) conducts integrity supervision of a wide range of financial and other institutions. This specific supervision is based on the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*), the Pensions Act (*Pensioenwet – Pw*), the Trust Offices Supervision Act 2018 (*Wet toezicht trustkantoren 2018 – Wtt*) and the Sanctions Act 1977 (*Sanctiewet 1977 – SW*). The *Wwft* implements the European directives aimed at preventing money laundering and terrorist financing.[4] This European directive is based on the recommendations of the Financial Action Task Force (FATF).

The purpose of integrity supervision is, among other things, to prevent the use of the financial system for money laundering and terrorist financing purposes. Supervision of compliance with the *Wwft* has been assigned to DNB for the following types of institutions: banks, branches, life insurers, payment service providers and agents, electronic money institutions, crypto service providers[5], foreign exchange institutions, trust offices and institutions referred to in Section 1a(3)(a) of the *Wwft*.[6] These institutions must also comply with the *Sw*. Every party in the Netherlands must comply with the *Sw*. Certain institutions fall under the supervision of DNB, including pension funds and insurers.[7]

DNB is responsible for implementing and enforcing the *Wwft*. Enforcement takes place in conformity with the Enforcement Policy of the Netherlands Authority for the Financial Markets (AFM) and DNB on the basis of standards laid down in legislation and regulations.[8]

DNB drew up an initial guideline in 2011 on the recommendation of the FATF. This provided institutions supervised by DNB with guidance to enable them to comply with the statutory obligations arising from the integrity regulations. This fifth edition of the Guideline incorporates a number of changes in the light of relevant amendments to the *Wwft* which came into force in 2020, except for the insertion of Section 3A of the *Wwft*.[9] The amendment of the *Wwft* on 21 May 2020 introduced a registration obligation for providers of services for exchange between virtual and regular currencies and providers of custodian wallets.[10] The

4 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
5 The institutions referred to in Section 23b of the *Wwft*: providers of services for exchange between virtual and regular currencies and providers of custodian wallets.
6 The *Wwft* refers to parties other than banks whose principal business is performing one or more of the activities included in points 2, 3, 5, 6, 9, 10, 12 and 14 of Annex I to the Capital Requirements Directive.
7 Article 1 of the Designation of Legal Persons under the Sanctions Act 1977 refers to Section 10(2)(a), (c) and (e) to (j) inclusive of the Sanctions Act 1977.
8 See also: https://www.dnb.nl/en/sector-information/supervision-laws-and-regulations/laws-and-eu-regulations/enforcement/
9 See: Bulletin of Acts and Decrees (Stb.) 2019, 265, Stb. 2020, 146, Stb. 2020, 231 and Stb. 2020, 380.
10 Stb. 2020, 146.

respective provisions are part of Section 3A of the Wwft. These provisions are not covered within the scope of this Guideline.[11]

In addition to the incorporation of relevant legislative changes, new Good Practices have been added to some sections, which have emerged from DNB's supervision investigations in recent years.

This Guideline is neither a legally binding document nor a DNB policy rule as referred to in Section 1:3(4) of the General Administrative Law Act (Algemene wet bestuursrecht) and does not have or aim to have any legal effect. This Guideline does not replace legislation and regulations, policy rules or supervisory regulations in this area. The examples in this Guideline are not exhaustive and cannot be deemed sufficient for compliance with the legal requirements in all cases. DNB intends this Guideline to serve as an aid for the explanation and application of the legal obligations.

This Guideline applies to institutions that are subject to DNB supervision and complements the "General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft)" of the Ministry of Finance and the Ministry of Justice and Security,[12] and the "Guidance Financial Sanctions Regulation" of the Ministry of Finance.[13] The guidance documents clarify the various obligations arising from the Wwft and the Sw and provide tools for the implementation of these obligations. The other Wwft supervisory authorities also provide guidance for the institutions falling under their supervision.[14]

This Guideline refers to international (non-binding) guidance documents issued by the FATF, the European Banking Authority (EBA), the Basel Committee on Banking Supervision (BCBS) and the International Association of Insurance Supervisors (IAIS). Although the guidance documents issued by these organisations are usually focused on certain sectors, much of the information they contain is also useful to other sectors. In addition, the documents produced by the Wolfsberg Group can be useful for some institutions.[15]

11 This also applies to Section V of the Implementation Act for the amendment of the fourth anti-money laundering directive, Stb. 2020, 146.
12 Available for consultation at: https://www.rijksoverheid.nl/documenten/richtlijnen/2020/07/21/algemene-leidraad-wet-ter-voorkoming-van-witwassen-en-financieren-van-terrorisme-wwft (available in Dutch only).
13 Available for consultation at: https://www.rijksoverheid.nl/documenten/rapporten/2020/08/12/leidraad-financiele-sanctieregelgeving (available in Dutch only).
14 AFM, Tax Administration/Wwft Supervision Agency, Financial Supervision Agency, Gambling Authorities and the presidents of the Netherlands Bar.
15 The Wolfsberg Group is an association of eleven global banks that develops financial services industry standards for 'Know your Customer/KYC', anti-money laundering and anti-terrorist financing policies (https://www.wolfsberg-principles.com/).

Relevant laws and regulations

This document provides guidance for the following laws and regulations:

- Anti-Money Laundering and Anti-Terrorist Financing Act (*Wwft*)[16]
- Sanctions Act 1977 and Regulation on Supervision pursuant to the Sanctions Act 1977 (*Sw*)
- (EU) Regulation 2015/847 concerning information accompanying transfers of funds (WTR2)

16 Legal text of August 2019. The amendments made up to that month are included in this Guideline.

2 Organisation of operational management

2.1 Ethical operational management

The integrity of financial institutions is one of the pillars of trust and is thus a prerequisite for institutions' proper functioning. Integrity is also included as an explicit standard in the financial supervision regulations. Sections 3:10 and 3:17 of the *Wft*, Section 143 of the Pensions Act (*Pensioenwet – Pw*) and Section 14 of the Act on the Supervision of Trust Offices (*Wet toezicht trustkantoren – Wtt*) contain the statutory requirements for monitoring ethical operational management. The key requirement is that institutions must avoid becoming involved in acts that contravene the law or are regarded as improper by society, and that they must safeguard the integrity of their operational management. The control of integrity risks is central in the development of this standard. The regulations (Financial Supervision Act, Prudential Rules (Financial Supervision Act) Decree, Pensions Act, Act on the Supervision of Trust Offices, Anti-Money Laundering and Anti-Terrorist Financing Act and Sanctions Act) essentially prescribe a control framework for the management of integrity risks. This Guideline focuses on the control of integrity risks: money laundering, terrorist financing and violations of sanction regulations. Other subjects also fall within the definition of integrity risks, such as corruption, conflicts of interest, fraud and unethical tax-related conduct. These integrity risks are included in this Guideline to the extent that there is a relationship with money laundering and/or terrorist financing and compliance with *Wwft* obligations.

Various institutions that are subject to the *Wwft* also have obligations under other laws and supervisory provisions in the context of ethical operational management pursuant to the Financial Supervision Act, the Prudential Rules (Financial Supervision Act) Decree, the Pensions Act and the Act on the Supervision of Trust Offices. This determines the scope of the control measures that institutions take to control their integrity risks. The measures that an institution takes to prevent involvement in money laundering and terrorist financing are part of this.

Integrity of directors and employees

Attention to the integrity of directors and employees is at least as important as the setting up of adequate processes, procedures and measures to mitigate the integrity risks of an institution. DNB's Policy Rule on Fitness stipulates that day-to-day institutional policymakers must among other things be fit in terms of ethical operational management and thus able to guarantee that the institution controls integrity risks. These day-to-day policymakers therefore carry primary responsibility within the institution for overseeing the existence, design and effectiveness of the integrity policy. Tools to help them do this include mission statements, business principles and strategic reviews. The day-to-day policymakers also ensure that the institution does not accept any customers or provide products and services of which the institution has no knowledge or experience. They also ensure that sufficient account is taken of the integrity risks during the development of new products and services and prior to their introduction. Finally, they also approve codes of conduct, procedures and measures that limit and effectively control the risks of money laundering, terrorist financing and violations of sanctions regulations and other relevant integrity risks.

The control framework for integrity risks comprises at least the following

- A systematic integrity risk analysis (SIRA), including the risks of money laundering and terrorist financing;[17] (See also: Section 2b of the *Wwft*);
- The determination of risk appetite based on the analysis of integrity risks including the risks of money laundering and terrorist financing;
- Adoption of an appropriate policy or group policy aimed at risk control and ethical conduct;
- The development and implementation of policy principles in codes of conduct, procedures and measures (see also: Section 2c of the *Wwft*);
- Systematic testing and assessment of the adequacy of the control environment, if necessary followed by modifications to that control environment;
- The establishment of a compliance function to the extent appropriate to the nature and size of the institution. (see also: Section 2d of the *Wwft*);
- Ensuring the exercise of an independent audit function for its work to the extent appropriate to the nature and size of the institution. (See also: Section 2d of the *Wwft*);

Responsible Wwft policymaker

On the basis of Section 2d(1) of the *Wwft* an institution with two or more policymakers must appoint a day-to-day policymaker who is responsible for compliance with the *Wwft*. The designated policymaker is the de facto '*Wwft* portfolio holder'. Having regard to this responsibility, a *Wwft* policymaker is always sufficiently informed of the integrity policy and the associated procedures of the institution. The *Wwft* policymaker actively maintains compliance with the relevant legislation and bears responsibility for implementing the institution's own policy. Finally, the *Wwft* policymaker receives relevant training and can demonstrate this when required.

17 Institutions that are only subject to the *Wwft* produce a systematic analysis of the risks of money laundering and terrorist financing under Section 2b of the *Wwft*. The SIRA system as described in Chapter 3 is used for this.

DNB Supervisory Strategy 2021–2024: A hard stance against financial and economic crime

Financial and economic crime comes in many forms, such as money laundering, corruption, terrorist financing, insider trading and non-compliance with sanctions. Combating these crimes is one of our key priorities, as they can harm confidence in the financial system. As "gatekeepers" to the financial system, financial institutions play a crucial role in detecting and preventing criminal cash flows.

Those institutions that do take appropriate measures to prevent financial and economic crime often also demonstrate ownership of the gatekeeper role. They are aware of the risks to which they are exposed and are prepared to identify, analyse and mitigate them using the three lines of defence model. This is why DNB encourages institutions and boards to take responsibility and prevent themselves from becoming involved in financial and economic crime. However, supervisory practice shows that ownership is often limited to the compliance function, and to a lesser degree the audit function. Robust lines of defence are required, with the management clearly bearing ultimate responsibility.

More information on DNB's Supervisory Strategy 2021-2024

2.2 Training and awareness

The operation of the *Wwft* and *Sw* processes and procedures in institutions mainly depends on the degree of awareness, experience and knowledge among day-to-day policymakers and employees. Adequate awareness, knowledge and experience on the part of institutions' staff concerning control of the risks of money laundering and terrorist financing are therefore important preconditions for an effective control framework. Staff training is an important tool to communicate and safeguard knowledge of the *Wwft* and the *Sw*, the principles of the integrity policy and procedures within the institution. In our supervision, we assess the extent to which institutions systematically fulfil the provisions of Section 35 of the *Wwft*.

Institutions provide training courses to familiarise staff with the provisions of the *Wwft* and the *Sw* and to enable staff to perform full and proper customer due diligence, recognise unusual transactions and ensure effective compliance with sanctions regulations. These training courses must cover, for example, money laundering and terrorist financing techniques, methods and trends, the international context and standards and new developments in the field.

As the integrity risks are dynamic and the control of institutions is adapted accordingly, it is necessary for institutions to evaluate and review the content of their training on a regular basis. To enable staff to keep abreast of new developments and to improve awareness in the long term, an institution must provide training programmes at regular intervals

rather than in one-off sessions. The frequency of the training depends on the purpose, target group and content. The types of training that institutions provide is therefore aligned with this requirement. Institutions may consider, for example, certified training courses, in-house training, e-learning modules and awareness sessions.

In order to design training as effectively as possible, it is important to focus the programmes on the different functions within the institution. The content, depth and frequency will thus depend on the employee's position. It makes sense if the compliance staff also take part in additional training to stay abreast of developments relating to international law and regulations and the risks of money laundering and terrorist financing. The day-to-day policymakers – who are entrusted with responsibility for compliance with the *Wwft* and *Sw* – must receive sufficient training to fulfil their responsibility or ultimate responsibility.

An appropriate record of the training provision, the courses taken, the frequency and participants enables institutions to determine and monitor the knowledge level in the organisation on an ongoing basis and to respond accordingly.

2.3 Ethical business culture

An ethical business culture and ethical conduct are vital for the effectiveness of integrity control measures. Ethical conduct is a professional, individual responsibility in which a person is aware of and takes proper account of the rights, interests and wishes of other stakeholders, displays an open and transparent attitude and is willing to take responsibility and render account for his or her decisions and actions. An ethical culture denotes a climate and atmosphere in which a company behaves or acts, including in a broader sense, in a way that it can explain and account for, respecting not only the letter but also the spirit of the law.

2.4 Internal whistleblower scheme and integrity reporting desk

Under Section 20a(1) of the *Wwft*, institutions must have procedures appropriate to their nature and size that enable employees to file internal reports of any violations committed by the institution. The person reporting the *Wwft* violations must be able to do so independently and anonymously. Section 20a of the *Wwft* is aligned with the provisions of the Dutch Whistleblowers Authority Act (*Wet Huis voor klokkenluiders*), under which employers must enable employees to file reports internally.

Individuals can also report misconduct to DNB's Integrity Reporting Desk. Professionals working in the financial sector may witness instances of fraud, corruption or other serious breaches of laws and regulations in a financial institution. DNB expects them to report misconduct in the first place internally to the institution they work for, for example by using an internal whistleblower scheme (such as one based on Section 20a of the *Wwft*). DNB's Integrity Reporting Desk will nevertheless deal with reports that cannot be filed directly with the institution concerned. This may be the case, for

example, if there is a well-founded fear of serious personal consequences. It is possible that an internal report has already been filed with the institution, but that the institution's response has been lacking or inadequate.

More information on the internal whistleblower scheme
More information on DNB's Integrity Reporting Desk.

2.5 Know your customer (KYC) / Customer due diligence (CDD)

Part of ethical operational management is customer due diligence. In order to guarantee ethical operational management, it is essential that institutions know who they are doing business with or who they are conducting an occasional transaction for. The *Wft* and the *Wwft* therefore require institutions to operate an adequate CDD system in order to know their customers and avoid entering into business relationships with persons who could damage trust in the institution. CDD standards are relevant not only for ensuring the ethical operational management of institutions as a whole, but also for controlling the specific integrity risks to which the *Wwft* relates. Since both the *Wft* (ethical operational management) and the *Wwft* are intended to control integrity risks, the measures taken by institutions under these Acts are integrated and the requirements of the *Wwft* and the *Wft* can be fulfilled in the same way.[18] The principal aim is that the institution knows who it is doing business with and the purpose of the business relationship, and continually monitors this to an extent commensurate with the risk. For further details see Chapter 4 'Customer due diligence' and Chapter 5 'Transaction monitoring and reporting unusual transactions'.

2.6 Sanctions regulations

The *Sw* and the regulations derived from it transpose international sanction regimes of the United Nations and the European Union into Dutch law. The provisions in these international sanction regimes are transposed into nationally applicable standards through the *Sw*. Non-compliance with the provisions adopted in or pursuant to the *Sw*, which may include international sanctions regimes, is punishable under the Economic Offences Act. The emphasis is on making it a criminal offence to contravene provisions enshrined in European Regulations.

The Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling Toezicht Sanctiewet 1977*) of the Netherlands Authority for the Financial Markets (AFM) and DNB gives financial institutions a framework for taking measures. There are two types of financial sanctions: orders to freeze assets, and bans or restrictions on the provision of financial services. These sanctions are intended to

18 See the letter from the Minister of Finance to the Dutch House of Representatives dated 15 October 2008 (Parliamentary Paper 31237, no. 9)

prevent undesirable transactions (embargoes) and to combat terrorism. Institutions take measures to ensure that they can identify relationships that correspond to legal or natural persons and entities as referred to in the sanctions regulations. Institutions subsequently ensure that they do not provide financial resources or services to the parties concerned and that they are able to freeze their financial assets. Chapter 7 provides more details of the sanctions regulations.

2.7 Foreign branches and subsidiaries of Dutch institutions

Under Section 2 of the *Wwft* an institution having a branch or a majority-owned subsidiary (or subsidiaries) outside the European Union or the European Economic Area (in a state in which the legal provisions to prevent money laundering and terrorist financing are less far-reaching than those of the *Wwft*) must ensure that its branch or subsidiary complies with the *Wwft*. International institutions with a registered office in the Netherlands must define the group policy and procedures for compliance with the *Wwft* that apply to the entire group. These institutions must also ensure that the group policy and procedures are enforced effectively. This means that the integrity control measures are applied in any event to all operational management, all functional activities and all customers and products worldwide.

An institution may operate in jurisdictions (non-EU Member States) where the local laws and regulations impose less far-reaching requirements than the adopted group policy. Institutions will then apply the group's more far-reaching requirements to those branches and subsidiaries. If the local laws and regulations impose more far-reaching requirements on integrity control measures than the group policy, the institution must adhere to the national legislation and adapt the group policy to local requirements. Finally, local legislation in a non-EU Member State may impede compliance with the *Wwft*. If institutions observe such cases, they must report them to DNB and take measures to ensure effective control of the potential risks.

Regulatory technical standards: impediments in third countries

On 3 September 2019 the 'Regulatory Technical Standards' (RTS) came into force concerning 'the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries'.

These RTS describe situations of possible legal impediments which institutions in non-EU Member States may encounter, how they should deal with them and how any impediment should be reported. Institutions must report such legal impediments to DNB.

3 Risk-based thinking: the systematic integrity risk analysis

3.1 Organisation of integrity policy

The regulatory framework for an appropriate integrity policy and, more specifically, for controlling the risk of money laundering and terrorist financing, is risk-based. This means that institutions apply the measures prescribed by law, and the intensity with which they do so is geared to the risks associated with certain customers (including the customer's ultimate beneficial owner (UBO)), products, transactions, services, delivery channels (the way in which contact is generally maintained with the customer) and country and geography. With regard to these risks there are factors that indicate higher risk of money laundering and terrorist financing; these are known as the risk factors (further details can be found in Chapter 3.3).

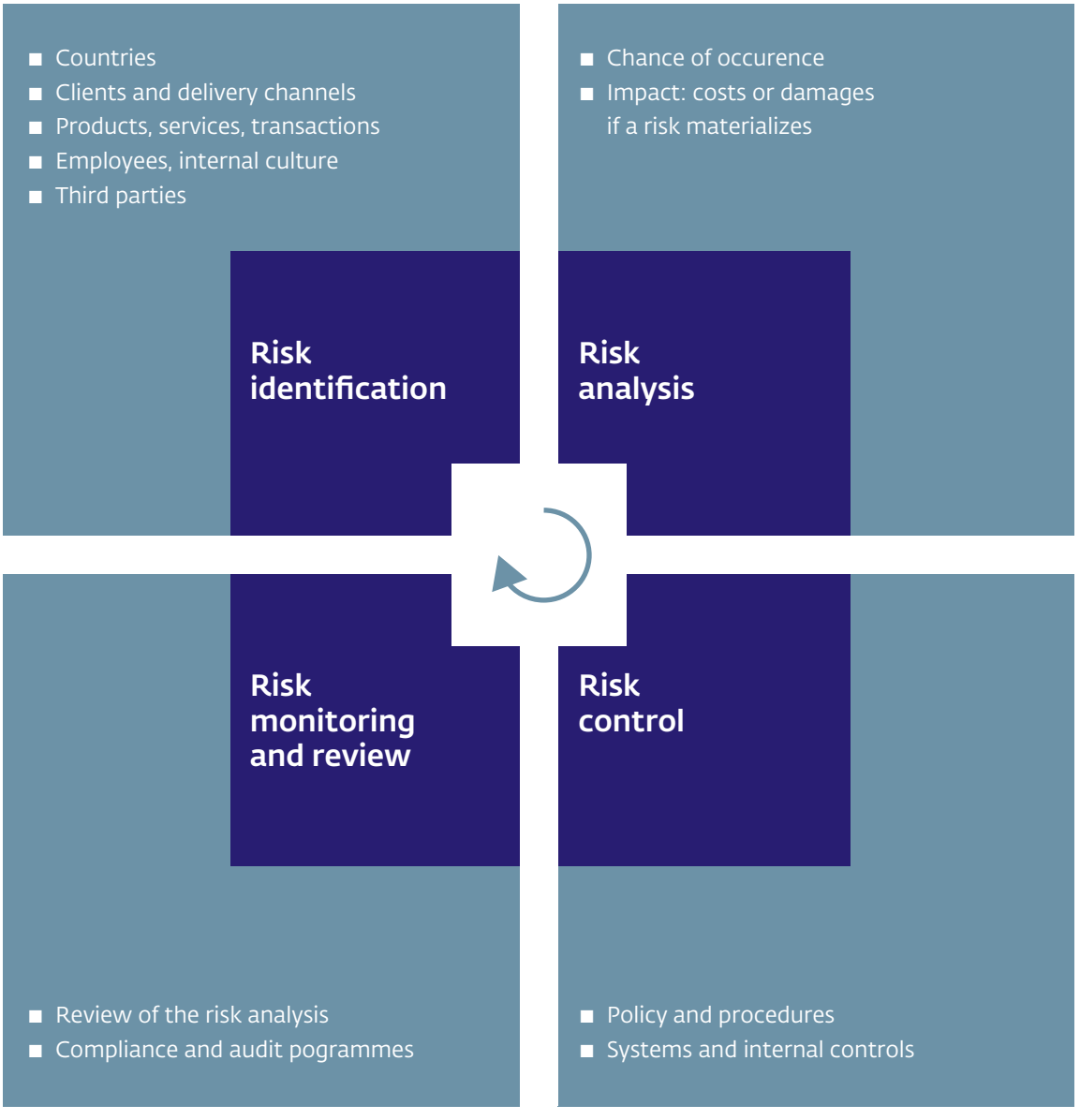
The framework of the *Wft* (which requires ethical operational management) and the *Wwft* assumes that institutions divide customers into risk categories based on the nature and extent of the risk. This stresses the individual responsibility of institutions: they assess the relevant risks themselves and then take appropriate measures to mitigate them. These risk categories range from low to high risk, and the classification is based on objective, identifiable factors. The higher the risks, the more effort the institution has to make to mitigate them (see 3.4 'Classification of customers in risk categories').

It is important that the institution conducts and records its deliberations in a systematic and consistent manner so they can be followed and assessed by a supervisory authority or other third party[19]. This applies both to the formulation of policy and to decisions to allow exceptions to that policy. In the performance of its supervisory duties DNB assesses the risk-based approach adopted by institutions.

3.2 Design of systematic integrity risk analysis (SIRA)

For institutions, preventing involvement in integrity violations, including money laundering and terrorist financing, begins with identifying the inherent integrity risks they incur, in part through the services they provide for customers. Inherent risks are deemed to mean institutions' susceptibility to be used, for example, for money laundering and terrorist financing as a result of the services they provide. In order to recognise their vulnerabilities, and to accept them (within the risk appetite) or to avoid them,[20] institutions must draw up a systematic analysis of the integrity risks (SIRA) and review them periodically. Drawing up a SIRA is an obligation that was initially imposed by the *Wft* but is now also included as an obligation in the *Wwft*. The risk analysis under the *Wwft* focuses on money laundering and terrorist financing, whereas the risk analysis under the *Wft* has a broader

19 Examples include parties with a controlling task such as the audit function.
20 See also the Good Practice entitled 'Integrity Risk Appetite'. Available for consultation at: https://www.dnb.nl/media/mkwlnn4w/brochure-good-practice-integrity-risk-appetite.pdf.


Countries
Clients and delivery channels
Products, services, transactions
Employees, internal culture
Third parties
Risk identification
Chance of occurence
Impact: costs or damages if a risk materializes
Risk analysis
Risk monitoring and review
Review of the risk analysis
Compliance and audit pogrammes
Risk control
Policy and procedures
Systems and internal controls

scope.[21] When drawing up the SIRA, institutions take account of the risk factors relevant to them. The SIRA means as a minimum that the institution performs the assessment periodically in accordance with a predetermined protocol. The institution then records the results of the assessment in writing.

The content of the SIRA depends on the organisation and activities of the institution concerned. A larger institution with complex services operating in international markets will have to contend with more risks than a smaller institution with simple services and straightforward products. The core term here is 'risk-based'. More information on drawing up a SIRA can be found in our *Good Practices* entitled "Integrity risk analysis – More where necessary, less where possible".

The assessment of integrity risks comprises four steps:

1. **Risk identification**: identifying the areas of service provision that are susceptible to integrity risks, such as money laundering or terrorist financing;
2. **Risk analysis**: performing a risk analysis to determine the likelihood and impact of integrity risks, such as money laundering or terrorist financing;
3. **Risk control**: drawing up and designing the risk control process; and
4. **Risk monitoring and review**: monitoring the risks and reviewing the risk analysis.

Good Practices – The Integrity Risk Analysis (SIRA)

In the Good Practices entitled 'The integrity risk analysis – more where necessary, less where possible' we provide practical tools for drawing up and implementing the SIRA.

Good Practices – Integrity Risk Appetite (SIRA)

These Good Practices include the main focal points for financial institutions wishing to survey their own integrity risk exposure and analyse the extent to which they wish to accept or avoid these risks.

3.3 Risk factors

The factors that entail an integrity risk relate to customers, services, products, transactions, delivery channels and country or geography and form the basis for the identification and assessment of integrity risks. When drawing up an integrity risk analysis, the institution looks first at the characteristics of its customers. These could include sectors or professions, residency, wealth, source of

21 Section 2b of the *Wwft* requires financial institutions to draw up a systematic risk analysis. This obligation applies to all institutions referred to in the *Wwft*. The obligation for certain financial institutions to conduct a systematic integrity risk analysis also results from Sections 3:10 and 3:17 of the *Wft*, Article 10 of the Prudential Rules (Financial Supervision Act) Decree, Article 19 of the Decree on the Financial Assessment Framework for Pension Funds and Article 14 of the Pensions Act Implementation Decree. For the latter institutions the SIRA has broader scope with the use of the umbrella term of integrity risks. See also the description in Chapter 2.1.

income and tax integrity risks.[22] It also looks at how the contact with customers is generally established and how services are offered (the 'delivery channels', e.g. in person, through intermediaries, by telephone or online). Finally, country or geography plays a role, in terms of the countries and regions in which the institution operates and the countries in which its customers are established or conduct their activities.

The application of the risk factors also enables the institution to classify its customers into risk categories. The institution looks not only at risk factors relating to the customer but also at a combination of factors affecting, for example, the product, service, transaction, delivery channel, country or geography (see Chapter 3.4).

When identifying the risk, institutions apply the risk factors of relevance to them. They then estimate the level of their risks. Each institution then assesses the likelihood of a particular risk of money laundering or terrorist financing manifesting itself and what the impact of such an eventuality would be. The weight assigned by an institution to each risk factor in determining the overall risk of money laundering and terrorist financing may vary depending on the institution. It is important that institutions assess the risk factors independently, taking due account of laws and regulations, as the *Wwft* considers that certain types of customers (such as PEPs) or certain types of services (such as services to correspondents) by definition represent a high risk.

The identified integrity risks are of course not static but dynamic. An institution's risky activities may change, for example. Certain trends can also arise within financial and economic transactions, and laws and regulations can also change. The SIRA is therefore also a living document that is regularly adapted to the latest internal and external developments and the institution's risk appetite.

Some examples of risk factors are provided below. This list of risk factors is not exhaustive and is generic in nature. This means on the one hand that institutions themselves must be alert to other factors indicating the risk level. On the other hand it is possible that the institution will conclude that certain factors do not apply to their situation or have already been sufficiently mitigated. For more examples DNB refers institutions to the Risk Factors Guidelines' compiled jointly by the European supervisory authorities in the financial markets (European Banking Authority, European Securities and Markets Authority and European Insurance and Occupational Pensions Authority). These guidelines contain more details of relevant risk factors relating to money laundering and terrorist financing in each financial sector.

22 Tax integrity risks refer to the risk of facilitating tax evasion and associated money laundering risk. Read more about tax integrity risks in our Good Practices concerning the tax integrity risk of banks and the Good Practices concerning the tax integrity risks of trust offices. Available for consultation at: https://www.dnb.nl/actueel/nieuws-toezicht/toezicht-nieuwsberichten-2019/publicatie-good-practices-fiscale-integriteitsrisico-s/ (available in Dutch only) and https://www.dnb.nl/voor-de-sector/open-boek-toezicht-sectoren/trustkantoren/integriteitstoezicht/good-practices-fiscale-integriteitsrisico-s-voor-clienten-van-trustkantoren/ (available in Dutch only).

Possible risk factors with regard to customers, services, products, transactions and delivery channels and country or geography

For detailed risk factors relevant to various sectors see the 'Risk Factors Guidelines' of the European Supervisory Authorities (EBA, ESMA and EIOPA).

Annexes II and III to the fourth Anti-Money Laundering Directive set out factors indicating a potentially lower and potentially higher risk.

In its 'interpretive note' the FATF cites examples of risk factors in Recommendation 10 (Customer Due Diligence). See the FATF website for its Recommendations.

The Financial Action Taskforce identifies countries in which deficiencies have been observed in the combating of money laundering and terrorist financing. The 'High-risk and other monitored jurisdictions'. See the FATF website for the up-to-date list of countries.

The European Commission identifies countries in which deficiencies have been observed in the combating of money laundering and terrorist financing. See the website 'EU Policy on High-Risk Third Countries' for the up-to-date list of countries.

Finally, the European Commission maintains a list of 'non-cooperative jurisdictions for tax purposes'. Countries that fail adequately to combat tax fraud, tax evasion and tax avoidance.

Section 2c requires institutions to take the risks referred to in the supranational risk assessment and the national risk assessment into account in their codes of conduct, procedures and measures. The European Commission issues a two-yearly 'Supranational Risk Assessment' (SNRA) setting out the major money laundering and terrorist financing risks to the European Union. The Ministry of Finance and the Ministry of Justice and Security also periodically issue two 'National Risk Assessments' (NRAs) describing the major money laundering and terrorist financing risks to the Netherlands.[23]

A separate NRA is issued for the Caribbean islands of Bonaire, Sint Eustatius and Saba.

23 The latest version of the National Risk Assessments can be found on the website of the WODC (Research and Documentation Centre) at https://www.wodc.nl/.

(Supra)national Risk Assessment

For European and national money laundering and terrorism risks see the 'Supra-National Risk Assessment' on the website of the European Commission and the 'National Risk Assessments' on the website of the WODC (Research and Documentation Centre).

3.4 Classification of customers into risk categories

Having performed the risk assessment, the institution then draws up an integrity policy and associated procedures. As part of this policy, the institution specifies the manner in which it divides its entire customer base into risk categories. The institution takes into account all factors (see 3.3 Risk factors) that could affect the integrity risk posed by a business relationship with a customer.

The institution documents the customer classification system in writing, for example in its customer acceptance policy. The institution itself decides how many risk categories are used and ensures that the policy is consistent with the nature, size and complexity of the institution's risk factors. This may mean that an institution that provides different services to different customer groups has more risk levels in its classification. The frequency of reviews of customer files is determined in accordance with the risk categories used by the institution. If there are grounds to do so, for example due to changes in the customer's circumstances, an 'event-driven' review of the customer file may also be carried out. An institution determines the circumstances under which an event-driven review takes place. The institution is responsible for keeping its customer files up to date.[24] An institution must take reasonable measures to ensure that the data are kept up to date. These are data collected pursuant to Section 3(2) to (4) concerning persons referred to therein. If an institution only uses the 'event-driven' review of the customer files, it must of course be able to demonstrate that the scenarios giving rise to an 'event-driven' review are sufficiently effective.

Under Section 3(11) of the *Wwft* the data in the customer file must be updated in any event if:

- relevant circumstances of the customer change,
- an institution is obliged under this Act to contact the customer in order to evaluate information relating to the ultimate beneficial owner, or
- the institution is obliged to do so under Directive 2011/16/EU on administrative cooperation in the field of taxation.

As well as classifying customers into risk categories, institutions must draw up a risk profile of an individual customer and use it among other things to monitor the relationship. The relevant risk factors are taken into account when drawing up

24 Section 3(11) of the *Wwft*. In addition, as part of their simplified customer due diligence and enhanced customer due diligence, institutions are required to maintain up-to-date data under Sections 6(3) and 8(11) of the *Wwft*.

a risk profile of the customer. An institution must understand the rationale for and appropriateness of the transactions and products for that customer so that any signs of money laundering and terrorist financing are conspicuous. For further information see Chapter 5.

The services and products provided by an institution can also be classified according to risk. Some products inherently carry a greater integrity risk. Generally, simple products and products offering long-term benefit accrual carry an inherently lower integrity risk than complex and short-term products. But these are only rules of thumb; the integrity risk is assessed for each product, and other risk factors, such as the country and the delivery channel, are also taken into account. In addition to the risk categories referred to here, the institution also takes account of other, new risks, such as those that may arise due to the use of new technologies.

The risk indicators that can arise in the business relationship with a customer include the following:

- the reason for opening the account or entering into the relationship;
- the amounts to be deposited by the customer or the size or purpose of the transactions to be effected;
- the extent to which and the way in which a customer is subject to specific supervision (e.g. a financial institution);
- the intensity and duration of the customer relationship;
- the customer's background, such as residence in a geographic area with lower or higher risk of money laundering and/or terrorist financing;
- the use of 'corporate vehicles' or other structures that have no demonstrable commercial or other purpose and entail complexity or lack of transparency;
- fiscal risk indicators. For this see the DNB Good Practices for tax integrity risks of banks[25] and trust offices[26].

The fourth Anti-Money Laundering Directive contains non-exhaustive lists of potentially lower and higher risk factors.

25 The Good Practices for tax integrity risks for customers of banks can be consulted at: https://www.dnb.nl/actueel/nieuws-toezicht/toezicht-nieuwsberichten-2019/publicatie-good-practices-fiscale-integriteitsrisico-s/ (available in Dutch only).

26 The Good Practices for tax integrity risks for customers of trust offices can be consulted at: https://www.dnb.nl/voor-de-sector/open-boek-toezicht-sectoren/trustkantoren/integriteitstoezicht/good-practices-fiscale-integriteitsrisico-s-voor-clienten-van-trustkantoren/ (available in Dutch only).

Example of risk classification

Risk category	Expamples	Review frequency review
Low risk	■ standard services for private customers (savings accounts, salary accounts, small credit card payments, etc.) ■ standard services for small business customers (current account facilities, etc.) ■ life insurance with a low annual premium or a low single premium ■ pension products	For example every three to five years
Moderate risk	■ accounts and routine international documentary or other payments for large and medium-sized companies ■ routine and standard private banking products and services ■ correspondent bank accounts for banks subject to legislation equivalent to the *Wwft*	For example two to three years
High risk	■ complex structured financing transactions or collateral arrangements with private customers ■ PEPs or customers conducting transactions involving PEPs ■ bank products and services that by their nature are susceptible to inappropriate use (e.g. back-to-back loans, large cash deposits, commercial real-estate activities) ■ customers with transactions to/from countries that are subject to sanctions (including trade sanctions), free trade zones, offshore centres, tax havens and countries which appear on the FATF watch list as part of the ICRG process ■ customers with frequent, non-routine, complex treasury and private banking products and services ■ non-routine, cross-border payments by non-customers ■ correspondent bank accounts with banks in jurisdictions with weak laws to combat money laundering and terrorist financing	For example annually

3.5 Customers and products with a heightened integrity risk

Certain types of customers or products may inherently carry a heightened integrity risk. These types can come to light in an institution's own risk analysis. Examples are companies with large amounts of incoming cash whose provenance is less easy to determine. For these kinds of customers the institution must take additional measures to mitigate the integrity risk. Cash is not the only form of currency whose provenance is less easy to determine. New payment methods such as cryptocurrencies also make it difficult to ascertain the provenance of assets.

Another example of possible heightened risk (including tax risk) is the combination of cross-border transactions and customers with a complex international company structure. The increased inherent risks associated with certain customers and products can be mitigated by taking measures. Measures to mitigate the heightened integrity risk include, for example, setting a limit on transactions, demanding more transparency from the customer and requiring the customer to make payments electronically. A heightened risk does not therefore necessarily mean that these types of customers have to be rejected.[27]

The European Commission identified certain factors indicating inherently heightened risk in Annex III to the fourth Anti-Money Laundering Directive. Section 8(2) of the *Wwft* states that institutions must at least take account of these risk factors. In addition to the risk factors stated in Annex III, DNB can also issue a policy statement identifying the activities in which it perceives heightened risk. Commercial real estate activities are a good example, because by their nature they carry a higher risk of fraud and money laundering due to the relatively high value of real estate, the often non-transparent pricing and the complexity of transactions. In 2011, DNB issued the Policy Rule 'Integrity Policy Regarding Commercial Real Estate Activities'. The Policy Rule states that institutions must have an adequate integrity policy in place to cover this heightened money laundering risk.

International Guidance and additional information: real estate and professional money laundering techniques

FATF, 'Money Laundering and Terrorist Financing through the real estate sector', 2007,
Financial Expertise Centre, 'Real estate reporting project', 2008,
Financial Expertise Centre, 'Red Flags for Real Estate Abuse - update 2010´', June 2010,

FATF, 'Professional Money Laundering', 2018

27 See also the letter from the Minister of Finance to the Dutch House of Representatives dated 18 January 2010 specifying the agreements entered into with the Dutch Banking Association (Nederlandse Vereniging van Banken – NVB) concerning payment facilities for integrity-sensitive sectors https://zoek.officielebekendmakingen.nl/kst-27863-35.html.

3.6 Unacceptable risks

On the basis of the customer due diligence and the defined risk profile, an institution may conclude that an existing or intended relationship with a customer entails excessive integrity risks. It can also occur that the customer due diligence procedure fails, for example due to a lack of necessary information, and the institution is thus unable to determine precisely who its customer is and/or what the purpose of the proposed business relationship is, and/or whether the intended service is appropriate. This may occur at the start of the relationship, but also during the relationship, if internal and/or external developments place increased demands on the customer acceptance process.

In the above cases the institution will not enter into a business relationship with the customer or will terminate an existing business relationship at the earliest opportunity. This obligation results from Section 5(3) of the *Wwft*. If there are indications that the customer is involved in money laundering or terrorist financing, it is required under Section 16(4) of the *Wwft* to notify the Financial Investigation Unit (FIU-NL). See Chapter 5.6 for more information. To ensure that all these obligations are met and that relationships with existing customers are terminated properly, the institution draws up a customer exit policy. Among other things, this policy states the circumstances under which the relationship with the customer will be terminated.

Examples of unacceptable risks:

- Problems in verifying the identity of the customer or the UBO
- Customers who wish to remain anonymous or who provide fictitious identity details
- Shell banks (banks incorporated and licensed in a jurisdiction where they have no physical presence)
- Customers appearing on a sanctions list
- Customers who, combined with the products they wish to acquire, present unacceptable risks on the basis of further information, e.g. from EVA, VIS or other sources
- Customers who are unwilling to provide full information (or are unable to provide adequate documentation to verify such information) concerning their nature and background, the purpose of the business relationship and in particular the source of their assets
- Customers whose organisational structure and/or the purpose of the structure of which the object company is a part is (are) found upon examination to be complex or non-transparent, having regard to the customer's activities, without there being a logical commercial explanation for this
- Professional counterparties who lack the required licences, referred to as illegal financial undertakings. Note: Both DNB and the AFM maintain public registers in which admitted financial institutions are entered. These registers can be used to check whether an institution holds a licence or registration.
- Existing or intended customers that give the institution insufficient information concerning structures, cash flows and/or tax motives.

4 Customer due diligence

4.1 Regulatory framework

The *Wwft* requires institutions to perform customer due diligence. An institution can largely determine the degree of customer research on the basis of risk.[28] This means the institution carries out customer due diligence in all cases, but that the intensity of the due diligence is determined wholly or partly by the risks associated with certain types of customers, products, services, delivery channels, transactions and countries or regions. Institutions must implement additional mitigating controls in cases that involve a heightened risk of money laundering or terrorist financing. This stresses the institution's own responsibility: the institution must make every effort to stay abreast of the techniques and methodologies used in money laundering and terrorist financing, the latest developments and relevant risk indicators, and must take these into account in its policy, procedures and measures.

The purpose of customer due diligence is to enable the institution:

- to identify its customers and verify their identity
- to identify the ultimate beneficial owners (UBOs) of a customer and take reasonable measures to verify their identity
- if the customer is a legal entity: to take reasonable measures to understand the ownership and control structure of the group to which a customer belongs
- to determine the purpose and intended nature of the business relationship
- to continuously monitor the business relationships and the transactions conducted during their existence to ensure that they are in line with the institution's knowledge of its customers and their risk profiles, where necessary carrying out further investigations into the source of the funds used in the relevant business relationship or transaction (see Chapter 5).
- to establish whether the natural person representing the customer is authorised to do so and, where relevant, to establish and verify that natural person's identity
- to take reasonable measures to verify whether the customer is acting on his own behalf or on behalf of a third party

28 The customer due diligence is covered by Sections 3 to 11 of the *Wwft*.

When entering into the relationship with the customer, the institution must therefore have gathered sufficient documents and information to accept the customer and achieve the above results. These must include at least the information and data listed in Section 33(2).[29]

The result of successful customer due diligence is that institutions know with whom they are doing business and all relevant risks have been identified. Institutions that do not establish their customers' identity beyond doubt consequently incur an unacceptably high risk of being used for money laundering or terrorist financing.

4.2 Identification and verification

4.2.1 General information

The *Wwft* uses a broad definition of the term 'customer'. The customer is the "natural or legal person with whom a business relationship is entered into or who has caused a transaction to be effected". A customer is any party with whom an institution enters into a business, professional or commercial relationship connected to the professional activities of the institution. The professional activities include the principal activities of an institution which, for example, are covered by its licence. However, if an institution performs other activities that have a financial component involving a risk of money laundering or terrorist financing, the institution must also apply the *Wwft* to those activities.

This broad definition also means that relationships maintained with professional counterparties as part of the institution's core activities fall within the scope of the *Wwft*, such as relationships between financial institutions (including correspondent relationships) and service providers.

For identification purposes, the customer must submit proof of identity. This can be done, for example, by submitting a paper or digital form. The verification process is intended to determine whether the submitted proof of identity matches the customer's real identity. On the basis of documents, data or information from credible and independent sources, the institution must verify the accuracy of the identity claimed by the customer. Section 4 of the *Wwft* Implementing Regulation lists a number of documents that can be used for this purpose. In the

29 a. for natural persons who are not ultimate beneficial owners as referred to in Section 1(1): 1°. the surname, first names, date of birth, the physical or registered office address of the customer and of the person acting on his or her behalf, or a copy of the document which includes a number identifying that person and on the basis of which identification has taken place; 2°. the type, number and date of issue of the document used to verify the identity;
b. of natural persons who are ultimate beneficial owners as referred to in Section 1(1): 1°. the identity, including at least the family name and first names of the ultimate beneficial owner; and 2°. the data and documents gathered on the basis of the reasonable measures taken to verify the identity of the ultimate beneficial owner;
c. for companies and other legal entities: 1°. the legal form, registered name, trade name, address and house number, postcode, place and country of registered office; 2°. in the case of a company or other legal entity registered with the Chamber of Commerce, the Chamber of Commerce registration number and the means by which the identity has been verified; 3°. in the case of those acting on behalf of the company or legal entity vis-à-vis the institution: the family name, first names and date of birth.
d. in the case of trusts or other legal structures: 1°. the purpose and nature of the trust or other legal structure; 2°. the law under which the trust or other legal structure is controlled.

case of legal entities, both the representatives and the customer must be identified. Further information on this can be found in 4.2.3.
Documents, information or data other than those specified in Article 4 of the *Wwft* Implementing Regulation can also be accepted for the purpose of verifying the identity of a natural person, provided they originate from a credible and independent source. It is the institution's responsibility to determine on the basis of its own risk assessment which documents, information or data are acceptable for the purpose of verifying a person's identity and accepting them as a customer. The institution's risk assessment takes account of the European Commission's list of high-risk third countries. See the website 'EU Policy on High-Risk Third Countries' for the up-to-date list of countries.

The identity of legal persons not established in the Netherlands is also verified on the basis of such documents, data or credible and independent information sources as are customary in international business. To this end documents can be requested that are comparable to those used to verify Dutch legal entities as described in Article 4(2) of the *Wwft* Implementing Regulation. The source of such documents must be sufficiently reliable and independent. This implies that the institution understands and assesses which sources are reliable and independent and the fact that these are legally recognised as means of identification in the customer's state of origin is deemed a relevant consideration in determining the reliability and independence. The European Commission's list of high-risk third countries is also taken into account in the acceptance of legal persons.

If documents do not originate from public authorities or the courts, the institution must question whether the documents are sufficiently reliable. Such documents will in themselves not be sufficient to verify a customer's identity. Documents that are generally not deemed to have been issued on the strength of adequate identification and verification include student cards, employee ID cards and copies of telecom or utility bills, for example. The 'one cent payment' procedure used by some institutions to verify identity is similarly not deemed to result from adequate prior identification and verification by another institution and should therefore not be regarded as a secure means of verifying a customer's identity. This means that other independent and reliable source(s) must be used in addition to this source.

An institution should always request additional documentation if it has any doubts whatsoever about the authenticity of any documents submitted.

4.2.2 Front men and representation

During the customer due diligence process, the institution also looks at whether the customer is acting for himself or for another party. The aim is to assess whether a person is acting as a front man on behalf of criminals or other third parties. If it is clear that a customer is acting for someone else, that third party qualifies as the customer ("the natural or legal person [...] who causes a transaction to be effected"), so the CDD obligations of the *Wwft* apply with regard to that person. In other cases a risk-based approach can be adopted: the institution takes reasonable measures to ascertain whether a person is acting for himself or for another party

(see Section 3(2)(f) of the *Wwft*. To this end an institution can define indicators to be used in the customer due diligence. These may include instances where the person is unable to answer certain questions, for example about the provenance of the funds, or where unclear, vague reasons are given for the transaction. If the institution suspects that the customer is a front man, this naturally constitutes a heightened or unacceptable risk.

When a natural person claims to be acting as a representative of a customer, institutions must also determine whether that person is authorised to do so. For legal entities, the representatives are often the board members. When a natural person claims to be representing a legal person indirectly (where the legal person is the customer), the chain of representative authority must be determined. An extract from the trade register, for example, may be used for this purpose. Once this authorisation has been established, the customer is the subject of the customer due diligence procedure set out in Section 3 of the *Wwft*. The natural person acting as representative must also be identified and his identity must be verified (see Section 3(2) preamble and (e) of the *Wwft*).

4.2.3 Unincorporated partnerships

A customer due diligence process comparable with that for legal persons is carried out for unincorporated partnerships. An unincorporated partnership can be described as a community of persons established by means of an agreement. An unincorporated partnership does not possess legal personality and is therefore not the party with which a business relationship is entered into or which causes a transaction to be effected. Examples include civil law partnerships, partnership firms, limited partnerships or similar communities of persons without legal personality, and comparable entities under foreign law. In a partnership firm, for example, the natural or legal persons who together constitute the partnership are deemed to be customers.

The institution identifies the partners and, where applicable, takes adequate, risk-based measures to verify their capacity as partners. An institution establishes which natural persons are able to exert material influence or have material interests, or exert a high degree of influence on the important decisions of the unincorporated partnership and who are able to exercise effective control over the policy of the unincorporated partnership. In the determination of the control structure, persons who are authorised to manage the partnership are also included in the customer due diligence, so the institution must identify them. The institution must take adequate, risk-based measures to verify the capacity of these persons to act as partners. Identity is verified on a risk basis in the case of natural persons who qualify as the equivalent of UBOs. Verification of the identity of all partners would be practically impossible in some cases, for example in the case of an open limited partnership.

4.2.4 Trusts

A trust is a foreign legal form that cannot be incorporated under Dutch law, but which is recognised in the Netherlands. It is also known as an 'Anglo-Saxon Trust'. Comparable legal structures are the French fiducie and the German Treuhand.

A trust (or other legal structure) does not possess legal personality and is therefore not the party with which a business relationship is entered into or that causes a transaction to be effected. Trusts therefore do not qualify as customers; the trustee is deemed to be the customer. The obligations under the *Wwft* therefore cover services provided for a trust. Where applicable the usual steps in the customer due diligence must be conducted, but the persons referred to in Section 3(1)(e) must also be known to the institution because they are considered to be the UBOs of the trust. The customer must state their identity, which must then be verified by the institution.

4.2.5 When identification and verification must be carried out

Section 3 of the *Wwft* specifies the cases in which customer due diligence must be performed. These are first and foremost cases in which an institution enters into a business relationship or conducts a transaction or a series of transactions above a specific limit.

Section 3(5)(b) of the *Wwft* stipulates that an institution must perform customer due diligence when two or more related transactions are conducted with a minimum combined value of €15,000. The institution will assess this on the basis of the type of transaction and the amounts involved. To begin with, they should be occasional transactions, which means that no business relationship needs to exists. It is assumed that the transactions will be similar in nature. For instance, someone who, through several transactions conducted in a few weeks or months, makes cash payments into an account of which he is not the holder (and not acting on behalf of the account holder) for a total amount exceeding €15,000. By contrast, this provision does not apply to a company that pays the cash proceeds from its regular operational management into its own account daily, as such payments are made as part of the business relationship.

Legislative history, however, indicates that a business relationship can be assumed to exist in the case of each individual money transfer[30]. Furthermore, since money transfers carry a high risk of money laundering and terrorist financing, institutions that conduct money transfer should always perform customer due diligence.

30 A transfer of funds within the meaning of Directive (EU) 2015/2366.

A customer due diligence procedure is carried out for all customers, including existing customers, if:

- there are indications that the customer is involved in money laundering or terrorist financing; such indications may be obtained, for example, from public sources ('bad press') or the monitoring of the transactions effected by the customer;
- the institution doubts the accuracy or completeness of information previously obtained from the customer;
- the risk of an existing customer's involvement in money laundering or terrorist financing gives cause to do so;
- there is a heightened risk of money laundering or terrorist financing due to the customer's country of residence;
  an occasional electronic money transfer[31] of at least €1,000 is made.

Identification and verification are completed before the business relationship is established and the service provision commences. Notwithstanding this, it is possible to verify the identity of the customer and, if applicable, the identity of the UBO when entering into the business relationship, if this is necessary to avoid disrupting the provision of service.[32] In such exceptional cases the purpose of the law should still be kept in mind, i.e. to prevent the institution's services from being used for money laundering or terrorist financing. The conditions are that the risk of money laundering and terrorist financing is low and that the identity is verified as soon as possible after the first contact with the customer. This could include situations where the nature of the institution or of the services offered creates technical or organisational reasons for initiating the provision of services on a limited basis. However, such initial service provision may take place only in low-risk situations. This means that the institution must perform a preliminary risk estimation to assess whether the risk of money laundering or terrorist financing is sufficiently low.

Institutions may also open an account in such cases, with verification of identity being carried out later, provided the institution ensures that the account cannot be used in the interim.[33] This also applies to credit cards issued by banks and authorised institutions. As long as the credit card is blocked (by analogy with an account that cannot yet be used), the institution can still perform verification, but once the credit card is unblocked and the card can be used (regardless of whether it is actually used), the identification and verification procedures must have been completed.

In addition to the above customer due diligence measures a financial undertaking acting in connection with a life assurance must, after designating the beneficiary, fulfil the obligations

31 As referred to in Article 3(9) of regulation (EU) 2015/847 of the European Parliament and the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) no. 1781/2006 (OJEU 2015, L 141).
32 Section 4(3) of the *Wwft*.
33 Section 4(4) of the *Wwft*.

included in Section 3(a) of the *Wwft*. The beneficiary's identity must be verified no later than the time of payout.

4.3 Entering into a business relationship

In principle an institution may enter into a business relationship only if it has completed its customer due diligence, if this has led to the intended result and if the institution has received all identification and verification information and other data. An institution does not need to perform the customer due diligence itself but can arrange for it to be carried out by another institution (the introducing party), which may be subject to the *Wwft*. [34] In that case an institution uses introductory customer due diligence as described in Section 5 of the *Wwft*.

If an institution engages a third party, which is not necessarily subject to the *Wwft*, in order to perform the customer due diligence (or parts of it), this constitutes outsourcing as described in Section 10 of the *Wwft*.[35]

4.3.1 Introductory customer due diligence

The responsibility for the customer due diligence and compliance with the *Wwft* obligations lies at all times with the accepting institution and not with the introducing party. The institution's responsibility extends not only to the obligations concerning the customer due diligence but also to compliance with the provisions relating to the recording of that due diligence. It should be noted that at the time of introduction an accepting institution must have access to the data used by the introducing institution in the customer due diligence.[36] The institution must also have access to the underlying documentation that has resulted in the acceptance of the customer. The accepting institution is also responsible for drawing up the risk profile and therefore requires the appropriate information. If the introducing institution cannot provide the information, the accepting institution will conduct the customer due diligence that is required under the *Wwft* or internal rules.

If the introducing institution has applied the simplified customer due diligence to a customer because this customer purchased a low-risk product, the accepting institution may request the introducing institution for more detailed identification and verification data commensurate with the risk associated with the customer at that time. An institution may always do more on the basis of its internal procedures than the *Wwft* requires, and may therefore also decide to perform customer due diligence itself. It goes without saying that the simplified customer due diligence is not an option if there is a suspicion of money laundering or terrorist financing. If the institution to which a customer is introduced has such a suspicion, it has additional grounds for requesting the data.

34 Section 5(1)(a) states which institutions can introduce customers.
35 It should be noted that the customer due diligence conducted as part of the ongoing monitoring of the business relationship and the transactions performed during the relationship cannot be outsourced.
36 Section 33(1) of the *Wwft*

An institution relying on the identification and verification of identity by another institution or party that is subject to the *Wwft* must proceed with care. As responsibility for maintaining an accurate customer file lies with the accepting institution itself, it is important that the institution ascertains that the relevant parts of the customer due diligence have been carried out in accordance with the *Wwft* (or comparable legislation in international situations) and that the other institution has adequate procedures and measures in place with regard to the *Wwft*. This means that the introducing party's procedures must be adequate in terms of their design and operation. An accepting institution cannot assume that the operation of such procedures and measures is adequate. If an institution repeatedly accepts customers from the same other institution, it would be logical for the former to request and assess the *Wwft* procedures of the latter in a risk-based way. In the case of collaborative arrangements the *Wwft* procedures should always be requested for assessment.

This is relevant in particular to life insurers who rely on customer due diligence performed by financial service providers acting as life insurance brokers. The insurer is responsible for proper implementation of the *Wwft* and the *Wwft* policy. Specifically, this means that the insurer formulates a customer identification and verification policy setting out the procedure in relation to reliance on customer identification and verification carried out by the relevant financial service providers. A policy is also formulated whereby the relevant financial services providers make customer identification data immediately available on request. Financial service providers acting as life insurance brokers have an independent obligation under the *Wwft*. In cases where the financial services provider has determined and verified the customer's identity,

When is the customer due diligence reviewed?

In the case of **low-risk customers**, in addition to the previously specified review time (as described in 3.4) a review can take place when:

- the customer requests a new service or product, or when customer contact presents an opportunity to conduct the customer due diligence;
- the characteristics of the customer change (e.g. relocation to a high-risk jurisdiction);
- alerts have been received relating to incidents or transactions.

For **high-risk customers**, a review will in practice be carried out more regularly (once or several times per year), for example in the case of:

- possible indications of heightened risk, such as the way in which accounts are used or specific transactions are conducted, in the context of the customer's consolidated position.

In all cases, the employees involved are aware of possible risks associated with this type of high-risk customer.

the insurer retains its own responsibility in this respect. For example, it may only write an insurance contract after ascertaining that the broker has determined and verified the customer's identity. Insurers must carry out periodic risk-based checks to ascertain whether the relevant financial service providers have measures in place to ensure proper application of customer due diligence. This can be done in various ways. For instance, the institution may annually request and assess the *Wwft* procedures used by a number of financial service providers acting as life insurance brokers. Other options are requesting an auditors' report (in particular for major financial services providers) or making random requests for a number of customer files.

4.3.2 Periodic update and review

On the basis of the customer due diligence the institution draws up a risk profile of the customer that falls into one of the risk categories defined by the institution (see section 3.4). This risk profile is dynamic, which means it may change over time. An institution therefore conducts a review of the customer due diligence to determine whether the customer still matches the defined risk profile. To that end the institution must periodically update the customer data, including the customer's risk profile, contact information and UBO(s). The basic principle is that the frequency and depth of the review depend on the risks presented by the customer. For this see also Sections 3.3 and 3.4.

In their policy and procedures institutions devote attention to the frequency and the way in which customer data is periodically updated. The customer's risk profile and the associated risk categorisation are key factors in this regard. In the light of the ongoing automation of CDD-related processes, the quality and quantity of the data and data fields is an increasingly important factor. Institutions take this into account specifically in the formulation of their policy. This concerns not only new customers but also the existing customer portfolio.

4.4 Not entering into or terminating the business relationship

This will prevent an institution concluding on the basis of the customer due diligence that an existing or intended customer carries excessively high risk of involvement in money laundering or terrorist financing. It can also occur that the customer due diligence procedure cannot be conducted in full, for example due to the lack of necessary customer information, and the institution cannot therefore determine precisely who its customer is and/or what the purpose of the intended business relationship is.

In both cases the institution will not enter into a business relationship with the customer[37] or will terminate an existing business relationship and conduct no transactions.[38]

37 Section 4(1) of the *Wwft* and Section 5(1) preamble and (b) of the *Wwft*
38 Section 5(3) of the *Wwft*

Under Section 5 of the *Wwft* it is prohibited to enter into a business relationship or conduct a transaction if no customer due diligence has been performed or if the customer due diligence, including the investigation of the UBO, has not produced the intended result. There is also a statutory obligation to terminate the business relationship if it is not possible to comply with the requirements relating to the customer due diligence.

If the institution also has indications that the customer is involved in money laundering or terrorist financing, it is required under Section 16(4) of the *Wwft* to notify the Financial Intelligence Unit (FIU-NL).

To ensure that all these obligations are met and that relationships with existing customers are terminated properly, the institution draws up a customer exit policy. Among other things, this policy states the circumstances under which the relationship with the customer will be terminated, and the procedure for doing so.

If the institution is unable to terminate the business relationship immediately, it must take appropriate or additional measures to perform the customer due diligence and must draw up a plan to terminate the relationship as soon as possible. Institutions may consider ring-fencing the service and applying enhanced monitoring until termination is possible. The key point is that the institution must make every effort to terminate the relationship and record such effort carefully.

4.4.1 Prohibition of business relationship in specific cases

It is not permitted to enter into or continue a correspondent relationship with a shell bank or another financial institution that is known to allow a shell bank to use its accounts.[39] Shell banks entail risks due to the nature of their organisation: they offer services in a country where they have no physical presence, which means they have no governance or management in that country. The conduct of such institutions is difficult for supervisory authorities to monitor.

In the case of a life insurance policy, where it is usually not legally possible to terminate an existing relationship, the assets are frozen until customer due diligence has produced the intended result.

4.4.2 Protected accounts

According to international standards on CDD and the combating of money laundering and terrorist financing, institutions are not permitted to maintain relationships with persons who remain anonymous or who provide fictitious identity details. Since in a limited number of cases it may be useful to protect a customer's identity internally – in order to protect the privacy and security of the customers involved and to prevent the use of inside information – the Regulation on Protected Accounts under the Financial Supervision Act[40] provides for a procedure

39 Section 5(5) of the *Wwft*. Shell banks are defined in Section 1a(1) of the *Wwft*.
40 See also: https://wetten.overheid.nl/BWBR0020672

in which the customer's identity is not visible or is otherwise protected during the processing of transactions. Although the customer is known to the institution, not all staff members are aware of his or her identity. The Regulation also allows the persons referred to in Section 44(1) of the Police Act and Section 15(2) of the Intelligence and Security Services Act to be provided with banking services.

Under this Regulation, banks or bank branches are permitted to make restrictive use of protected accounts. The Regulation describes the way in which banks and bank branches should maintain a central register in such a way that a customer's identity details are not visible or are otherwise protected during the processing of transactions, whilst being known elsewhere in the institution. The central register will contain the data to be recorded pursuant to Section 33 of the *Wwft*. The central register will be set up in such a manner that it can be searched by name and by number or code key. An administrator of the central register is also designated and the Compliance department has access to the register.

The Regulation thus relates only to the protection of identity during the processing of transactions. The requirements under the *Wwft* regarding customer due diligence remain fully applicable, as does the Regulation of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds.[41]

It is also relevant in this context to refer to accounts with a different name from the name of the customer or account holder, such as 'in name of' accounts. Although there can sometimes be a legitimate explanation for such accounts, for example in the case of insurers with different labels or brands, institutions should be particularly alert if a customer requests an 'in name of' account with an account name that cannot be explained. During the periodic review, it is possible that such an account will go unnoticed because of the different account name used. Using a different account name in this way can also be misleading for other institutions, for example when carrying out the name-number check or when assessing alerts from the transaction monitoring system.

4.5 Ultimate beneficial owner (UBO)

The customer due diligence includes the determination by the institution of the identity of the ultimate beneficial owner (UBO) (identification and verification). The institution must identify the UBO in respect of each customer. The ultimate beneficial owner is always a natural person. This rule is relevant not only when the customer is a legal entity, such as a legal person or foundation, or a legal structure such as a trust, but also when the customer is a natural person over whom another natural person has actual control or for whose account a transaction or activity is performed.[42]

41 See Chapter 6 of the Guideline for a explanation of this regulation.
42 See the definition of ultimate beneficial owner in Section 1(1) of the *Wwft*. Article 3 of the *Wwft* Implementation Decree 2018, stating which categories of natural persons must *in any case* be designated as the ultimate beneficial owners, is also important.

The customer due diligence concerning the UBO is a legal requirement.[43] The background to this is that criminals can use structures involving Dutch or foreign legal persons as a means of concealing the criminal origin of funds.

The requirement to identify the UBOs can usually be fulfilled by instructing the customer to declare who the UBO is. The institution then takes "reasonable measures" to verify the declared identity, as the truthfulness of the data provided by the customer has not been verified. The verification involves a risk assessment based on independent and reliable sources, such as public sources, an extract from the trade register or confirmation of the party's declaration by an independent third party. Pursuant to Section 4(2) of the *Wwft* the institution is obliged to obtain an extract from the UBO register[44] and to include it in the customer file. Verification cannot take place solely on the basis of the extract obtained.[45] An institution must always verify the identity of the UBO, regardless of the risk. His/her identity must always be verified, but the method and depth of the verification will be risk-based. This means that more extensive measures are taken in the case of high-risk customers than low-risk customers. The verification measures enable the institution to obtain sufficient information to convince itself of the identity of the UBO. In all cases the institution also checks whether the UBO is a PEP (Politically Exposed Person).

43 Section 3(2)(b) of the *Wwft*.
44 Section 15a of the Commercial Register Act states that a UBO register must be maintained. The second paragraph of that provision specifies the data that must be included in the register.
45 Section 3(15) of the Wwft.

Feedback obligation

Section 10c of the *Wwft* includes a 'feedback obligation'. If the institution ascertains that the UBO (or pseudo-UBO) data entered in the commercial register are incorrect or incomplete, it must report this to the Chamber of Commerce. This obligation does not apply if, under Section 16 of the *Wwft*, a report is filed with the FIU.

The introduction of the UBO register on 27 September 2020 is followed by an 18-month registration period. Companies and other legal entities have 18 months to enter their UBO data in the register. During that period the feedback obligation applies only if that registration has taken place and the institution identifies a discrepancy between the entered data and data available to it by other means. If a company or other legal entity has not registered any UBO data, the institution is not required to provide feedback.[46]

If the institution identifies a discrepancy and provides feedback, this does not generally mean that no business relationship can be entered into with the customer concerned. Any relationship is based on the overall result of the institution's own customer due diligence.

In specific cases a simplified customer due diligence can be applied to the investigation of the UBO(s). Annex II to the fourth Anti-Money Laundering Directive includes a non-exhaustive list of customer risk factors that potentially entail a lower risk. These factors are important for the overall customer due diligence (see section 4.8 below). Simplified customer due diligence does not mean that *no* examination is conducted.

Institutions must also have adequate risk-based measures in place to gain an insight into the customer's ownership and control structure in the case of legal persons, foundations, trusts and other legal structures. These include measures to verify the legal status of customers other than natural persons, if possible by obtaining proof of incorporation.[47] The basic principle is that the institution knows the relevant structure and understands it. This means that for complex structures consisting of many companies, the institution must expend more effort in order to understand the domestic or international shareholding and control structure of the organisation than for a Dutch private limited company (BV) with a majority shareholder-director. As part of these efforts, the institution examines the customer's reasons for using complex structures.

46 Section 57(3) of the Commercial Register Act.

47 This verification can take place as described in Annex 4 to the Guidelines – Sound Management of Risk Related to Money Laundering and Financing of Terrorism, Basel Committee on Banking Supervision. Available for consultation at: https://www.bis.org/bcbs/publ/d353.htm.

This can be done by making enquiries of the customer, but for example also by requesting a legal or tax opinion or advice. An understanding of the tax motives as part of the customer due diligence enables the institution to ascertain whether there are tax integrity risks. The examination of the ownership and control structure is closely linked to the examination of the purpose and nature of the relationship.[48]

Section 3 of the *Wwft* Implementation Decree 2018 lists a number of legal forms and specifies the natural persons who must be designated as UBOs in each case. This is a non-exhaustive list.

It follows from Article 3(1)(a)(2) of the *Wwft* Implementation Decree 2018 that it is sufficient for institutions to designate the senior management, for example the directors appointed under the articles of association, as the customer's UBO.[49] This fallback option, also known as the 'pseudo-UBO', can only be used if (a) the institution has exhausted all possible measures, (b) there are no grounds for suspicion and (c) the due diligence has not resulted in the identification of actual UBO(s) or an institution doubts whether the designated natural person is an actual UBO. This is an extreme fallback option that is only available in these cases.[50] Article 3(6) of the *Wwft* Implementation Decree 2018 states what is understood by senior management in this context. Section 3(2)(b) of the *Wwft* then includes a provision on the identification and verification of the UBO who is a member of the senior management.[51]

An essential part of the customer due diligence concerning the UBO is its recording. It goes without saying that an institution must record the measures taken to identify the natural person who is the UBO and, if applicable, what the rationale is for designating the senior management as the UBO. In the latter case (pseudo-UBO) an institution must therefore record accurately in the relevant customer file how it has fulfilled the two conditions (a and b above). If an institution departs from the procedures it has drawn up, it is important to have a record substantiating why it has done so in particular cases.

48 For further information see the DNB Good Practices for tax integrity risks with banking customers.
49 Article 3(1)(a)(2) of the Wwft Implementation Decree 2018, read in cojunction with the explanatory memorandum. Which can be found here: https://zoek.officielebekendmakingen.nl/stb-2018-241.html
50 Article 3(1)(a)(2) of the *Wwft* Implementation Decree 2018.
51 The Memorandum of Explanation provides as follows with regard to Section 3(2)(b): "The reason for explicitly including this obligation in the directive is that a member of the senior management can only be designated as the ultimate beneficial owner if, after all possible means have been exhausted, no other ultimate beneficial owner can be designated or if there is doubt as to whether the identified ultimate beneficial owner is indeed the ultimate beneficial owner."

Definition of UBO in Wwft Implementation Decree 2018

- In the case of BVs and NVs (with the exception of 'listed companies'), a UBO is the natural person who, directly or indirectly, has an economic interest amounting to more than 25% of the company or who controls the company.
- In the case of unincorporated partnerships, the UBO is the natural person who directly or indirectly has an ownership interest of more than 25% or who can exercise more than 25% of the votes in the case of corporate actions and/or amendments to the partnership agreement.
- In the case of foundations and associations, the UBO is the natural person who directly or indirectly has an ownership interest of more than 25% or can exercise more than 25% of the votes in the case of an amendment to the articles of association, or has de facto control of the legal entity.
- The Memorandum of Explanation accompanying the AMLD4 implementation act states that the 25% rule is intended to be indicative.[52] Persons with a lower percentage can also be designated as UBO if they have ultimate control by other means, for example in the case of a contractual relationship whereby such persons have ultimate control.
- In the case of a trust, several persons are designated as UBOs, including the settlor(s), the trustee(s), the protector(s), the beneficiary/beneficiaries, the group of persons in whose interest the trust was principally established.
- In the case of religious communities, the UBOs are the natural persons who are designated in the religious community's bylaws as the legal successor in the event of its dissolution.

For a full overview see Article 3 of the *Wwft* Implementation Decree 2018

4.6 Purpose and nature of business relationship

Gathering information about the purpose and intended nature of the business relationship enables an institution to estimate any risks that may arise from the provision of services for the customer. Generally, part of the required information will already have been obtained during the contact with the customer prior to the establishment of a business relationship. The purchased services or products may indicate the purpose of the relationship. The institution may ask additional questions to clarify the details concerning the user of the product or the recipient of the service. In the case of customers not residing or established in the Netherlands, an institution must be clear as to why the customer intends to use its services or

52 See also the Memorandum of Explanation (Parliamentary Papers II 2017/18, 34808, no. 3, p. 4): '(a) no person or persons can be identified who qualify (directly or indirectly) as UBO by means of shares, voting rights or ownership and no person or persons have been identified who have control by other means, or (b) cases in which there is doubt as to whether the identified persons are actually UBOs. It must be clear, however, that every possible effort has been made to identify the UBO(s) and there must be no grounds for suspicion of money laundering or terrorist financing.

products in the Netherlands. If it is for tax reasons, the institution will assess the acceptability of the position to ensure that no tax evasion is being facilitated and that no tax structures are being facilitated that fall outside the institution's risk appetite (aggressive tax planning). In such cases an institution can make this assessment on the basis of its risk analysis.[53] With regard to the purpose and nature of the relationship, the institution must also assess the type of transactions (e.g. quantity, frequency and size) that the customer intends to perform in situations of heightened risk.

4.7 Source of funds

Customer due diligence requires an institution to investigate the source of the funds used in a business relationship or transaction if necessary.
The institution must include statements and objective and independent documentary evidence of the source of funds in the customer file and make additional enquiries where necessary. The fact that the funds originate from a regulated institution does not mean that the institution itself is exempted from performing a due diligence review. To determine the plausibility that the funds originate from a legal source, the institution must identify specific indicators which determine the depth of the review. Possible combinations of indicators are the amount concerned, the stated explanation for the origin of the funds, the age and occupation or business activities of the customer, the country of origin or destination of the funds and the product or service supplied. In the case of life insurance, the indicators could be, for example, the level of the initial premium or any additional premiums. Specifically in case of high risk, it is appropriate to determine the plausibility of the origin of the funds using independent and reliable sources and to record this in the customer file. This also applies to private banking customers.

In order to verify the source of the funds used in the business relationship, it may also be necessary, especially with high-risk customers, to have an understanding of the customer's asset position. Where customers spread their assets, it is also necessary for the institution to be aware of the other assets in order to define a correct risk profile. The institution should document its review of the source of funds.

4.8 Simplified customer due diligence, low-risk factors and exceptions to the customer due diligence

For certain customers and transactions it is sufficient to conduct simplified customer due diligence under Section 6 of the *Wwft*. The conclusion that simplified customer due diligence is appropriate will always be based on a risk assessment. A risk assessment will take place in all cases, after which the intensity of the customer due diligence will be geared to the estimated risk. The institution can carry out a prior assessment of the cases in which simplified customer due diligence will be used. This will be done by means of a prior risk analysis, taking into account the risk

53 For more information see the DNB Good Practices on tax integrity risks for banks and trust offices.

factors on the basis of which the low-risk customers will be identified.
The institution's assessment must in any case include the non-exhaustive list of risk factors stated in Annex II to the fourth Anti-Money Laundering Directive. These factors indicate situations of 'potentially lower risk'. Listed companies and government institutions are cited as low-risk examples. This applies equally to listed companies and government institutions in other EU Member States and third countries that have effective legislation and supervision to combat money laundering and terrorist financing.

In addition to customer risk factors, there are also risk factors that indicate a potentially lower risk in the case of products, services, transactions and delivery channels. Here too Annex II to the fourth Anti-Money Laundering Directive provides a point of reference. Examples are products that cannot benefit third parties and whose benefits are accrued only in the long term, or products carrying a low risk of money laundering and terrorist financing due to spending limits or transparency of ownership. The list stated in Annex II is not exhaustive, so there may be other risk factors indicating a potentially lower risk. More detailed risk factors are stated in the 'Risk Factors Guidelines' produced jointly by the European supervisory authorities in the financial markets (EBA, ESMA and EIOPA). See also Chapter 3.3, which contains more references to risk factors. The 'Risk Factors Guidelines' provide examples of measures that can be taken as part of simplified customer due diligence.[54]

List of factors of potentially lower risk situations in Annex II to the fourth Anti-Money Laundering Directive

Customer risk factors

- public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;*
- public administrations or enterprises;
- customers that reside in geographical areas of lower risk as set out in point (3) in Annex II.

*for more information on listed companies and low risk see Section 4.5, Paragraph 4.[55]

54 See point 44 ff. of the Risk Factors Guidelines.
55 One of the specified customer risk factors concerns listed companies that are subject to information requirements (disclosure requirements). It is important that institutions do not merely assume that a listed customer will always entail lower risk. A relevant factor, for example, is the stock market on which the company is listed. The percentage of the share capital that is listed is also important; UBOs may also be among the holders of listed shares. Furthermore, the mere fact that a company is listed on a "recognised stock exchange" is not sufficient to decide to apply simplified customer due diligence. A risk analysis must therefore be made to assess the depth to which the customer due diligence can be carried out.

Product, service, transaction or delivery channel risk factors:

- life insurance policies for which the premium is low;
- insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
- a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
- financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
- products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).

Geographical risk factors:

- Member States;
- third countries having effective AML/CFT systems;
- third countries identified by credible sources as having a low level of corruption or other criminal activity;
- third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

One of the specified customer risk factors refers to listed companies that are subject to information requirements (disclosure requirements). The mere fact that a company is listed on a "recognised stock exchange" is not sufficient to decide to apply simplified customer due diligence. Institutions cannot merely assume that a listed customer will always entail lower risk. Non-customer risk factors may also play a role, for example the type of product, service or transaction and geographical risk factors. A relevant factor is the stock market on which the company is listed and the percentage of the free float is also important. The non-tradable part of the share capital is not excluded from the UBO investigation (see Section 4.5). A prior risk analysis must therefore be made to assess the depth to which the customer due diligence can be carried out for this type of customer.

By means of their risk assessment institutions can identify low-risk situations on a case-by-case basis. The risk assessment must in any event take account of the risk factors referred to in Annex II to the fourth Anti-Money Laundering Directive.

Institutions collect sufficient data to assess whether simplified customer due diligence will be sufficient for the customer concerned. For instance, the institution may request an extract from the Chamber of Commerce, entries in public registers or other public listings. The institution must keep the information on which the simplified customer due diligence is based up to date in accordance with Section 6(3) of the *Wwft*. Keeping the details up to date also means regular inspection to ascertain whether the risk remains low as previously ascertained. For customers on whom simplified customer due diligence has been conducted an institution will have sufficient data to fulfil its reporting requirement under Section 16 of the *Wwft*.

The institution must also assess whether the account is held and operated by the customer for his/her own use. For instance, banks sometimes hold an account in their own name with another institution, but the funds in that account belong to the bank's customer(s) and the transactions on the account are conducted for the account and risk of that customer or those customers. In these cases, the institution must consider whether the purpose of Section 6 of the *Wwft* (i.e. simplified customer due diligence due to low risk) is still being met or whether it must observe the provisions of Section 3 of the *Wwft* vis-à-vis the customer(s) for whose account and risk transactions are effected, or whether the relationship with the other bank must be treated as being of higher risk (pursuant to Section 8 of the *Wwft*).

Notwithstanding the application of Section 6, institutions must gather sufficient information to carry out their checks under sanctions law. Further information on sanctions regulations can be found in Chapter 7.

Section 7 of the *Wwft* contains a specific exception for certain parts of the CDD obligations described in Sections 3 and 4 of the *Wwft* with regard to business relationships and transactions involving electronic money. It should be noted that the exception is limited and subject to many conditions. This exception does not alter the fact that the obligation to conduct continuous monitoring of the business relationship (transaction monitoring) applies in full (Section 3(2)(d) of the *Wwft*). The exception provided for in Section 7(1) of the *Wwft* cannot be applied under certain circumstances. These concern the conversion of electronic money into cash and remote payment transactions (see Section 7(3) of the *Wwft* for the precise description).

4.9 Enhanced customer due diligence and high-risk factors

Section 8(1)(a) of the *Wwft* states that enhanced customer due diligence must take place if there is a heightened risk of money laundering and terrorist financing. Enhanced customer due diligence must always be applied in the following cases: (i) if the business relationship or transaction by its nature entails a higher risk of money laundering or terrorist financing or, (ii) if the customer is resident, established or has its registered office in a state designated by the European Commission under Article 9 of the fourth Anti-Money Laundering Directive as carrying a higher risk of money

laundering or terrorist financing.[56] The other paragraphs of Section 8 cite other cases in which enhanced customer due diligence must always take place, as in the case of Politically Exposed Persons.

An institution itself determines whether a situation is high-risk (and hence requires enhanced customer due diligence) by means of a risk assessment. In their risk assessment institutions take account of the list of (non-exhaustive) risk factors referred to in Annex III to the fourth Anti-Money Laundering Directive. These factors give institutions a basis on which to assess whether a situation is high-risk. The stated examples are not exhaustive, however; there may also be other factors indicating high risk. Institutions draw up policy and procedures on the basis of their risk assessment and identify the cases in which there is high risk, taking into account Annex III to the Directive. An example is a business relationship or remote transactions in which the customer is not physically present at the time of acceptance. More details are provided in 4.9.1 below.

In cases where the institution believes there is a heightened risk of money laundering or terrorist financing, the institution takes additional measures (i.e. in addition to those taken pursuant to Section 3 of the *Wwft*). These measures vary depending on the risk. The additional measures to be taken depend on the institution's risk assessment with regard to the customer, transaction, product and country concerned.

The *Wwft* also requires institutions to take reasonable measures to investigate the background and purpose of complex or unusually large transactions, transactions with unusual patterns and transactions that have no clear economic or lawful purpose. In such cases, the entire business relationship with the customer must be subjected to enhanced CDD.[57]

Non-exhaustive list of factors and types of evidence of potentially higher risk in Annex III to Directive 2015/849 as amended in Directive 2018/843

Customer risk factors:

- the business relationship is conducted in unusual circumstances;
- customers that are resident in geographical areas of higher risk as set out in point (3);
- legal persons or arrangements that are personal asset-holding vehicles;
- companies that have nominee shareholders or shares in bearer form;
- businesses that are cash-intensive;

56 In addition to the European Commission, the Financial Action Task Force operates a country list of 'High-risk and other monitored jurisdictions', which can be consulted at http://www.fatf-gafi.org/countries/.
57 Section 8(3) of the Wwft.

- the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
- customer is a third country national who applies for residence rights or citizenship in the Member State in exchange of capital transfers, purchase of property or government bonds, or investment in corporate entities in that Member State.

Product, service, transaction or delivery channel risk factors:

- private banking;
- products or transactions that might favour anonymity;
- non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) no. 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;
- payment received from unknown or unassociated third parties;
- new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;
- transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

Geographical risk factors:

- without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- countries identified by credible sources as having significant levels of corruption or other criminal activity;
- countries subject to sanctions, embargoes or similar measures issued by, for example, the Union or the United Nations;
- countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

High-risk customer, product, transaction and country

If jurisdictions have been identified by the European Commission and/or the FATF as jurisdictions that have deficiencies in their regimes for the combating of money laundering and terrorist financing, this should be regarded as one of the factors that increase the risk of money laundering and terrorist financing in a business relationship or transaction.[58] In such cases institutions must take additional measures to mitigate the heightened risk. If the customer is not a natural person, the institution must decide which measures to take to verify the legal status of that customer. The measures to be taken depend on the risk of the jurisdiction concerned. If a customer is a Dutch legal entity but has a UBO resident in such a state, this means that the institution must include this UBO as a high-risk factor.

Special measures are also taken for transactions and business relationships that are connected with these states, ranging from additional checks on business relationships and correspondent relationships to limiting or refusing to execute certain transactions.

Standard procedures are not sufficient when accepting customers purchasing a product with a heightened risk, for example products or combinations of products which differ from standard products. The institution must therefore do more than simply check whether the customer or other stakeholders appear(s) on the sanctions lists, whether they are creditworthy (e.g. through the Dutch Credit Registration Agency) or whether their identity documents are genuine (e.g. through the Dutch Identity Verification System) and whether the customer appears in institutions' internal or external warning systems. Such additional information may relate to the reputation of the customer or the UBO, but also of persons with whom they are associated. This includes the acquisition and assessment of information on business activities, including negative information. As part of enhanced customer due diligence, the institution must also conduct a deeper investigation into the source of the funds. Section 9(1) of the *Wwft* details the enhanced due diligence measures that institutions must take with regard to transactions, business relationships and correspondent banking relationships if these are related to states designated by the European Commission under Article 9 of the Fourth Anti-Money Laundering Directive. These designated states represent a higher risk of money laundering or terrorist financing.

58 See the DNB Q&A on FATF watch lists, available for consultation at: https://www.dnb.nl/en/sector-information/supervision-stages/regular-supervision/supervision-of-financial-crime-prevention-integrity-supervision/q-a-on-financial-action-task-force-warning-lists/.

The following enhanced measures must be taken pursuant to Section 9(1) of the *Wwft*:

- Collection of additional information on those customers and ultimate beneficial owners
- Collection of additional information relating to the purpose and nature of that business relationship
- Collection of information on the origin of the funds used in that business relationship or transaction and the source of the assets of those customers and of those ultimate beneficial owners
- Collection of information on the background to and motives for those customers' intended or executed transactions
- Obtaining senior management approval to enter into or continue that business relationship
- Enhanced monitoring of that business relationship with those customers, and of their transactions, by increasing the number of checks and the frequency of updates of data on those customers and those ultimate beneficial owners and by selecting transaction patterns for closer investigation.

4.9.1 Customer not physically present

Up to 25 July 2018, Section 8 of the *Wwft* required enhanced customer due diligence if the customer was not physically present during identification and verification of his or her identity. The risk of a non-face-to-face relationship is now included as one of the high-risk factors in Annex III to the directive. Section 8 of the *Wwft* refers to this annex. The result of this amendment is that institutions adopt a risk-based approach to determine which measures will be taken to compensate for the higher risk of a non-face-to-face relationship. A key point here is that institutions must not enter into any business relationship or conduct any transactions if the customer due diligence has not been completed in accordance with Sections 3, 5 and 8 of the *Wwft*. It is emphasised that the measures taken if the customer is not physically present under Section 8 are additional to the measures taken under Section 3. A non-face-to-face relationship with the customer and the application of innovative techniques are referred to as high-risk factors in Annex III. The fact that customers are accepted remotely through the use of innovative techniques does not mean they are by definition included in a high-risk classification following acceptance (see section 3.4).

An institution must determine whether the declared identity actually matches the identity of the person who presents himself or herself. Institutions must therefore be able to determine that the identity document belongs to the person who has not attended in person. They must know who they are doing business with. It will therefore also be insufficient to have two proofs of identity if it is not established that these actually belong to the potential customer. Multiple independent and reliable sources must be consulted. An institution will assess which sources are actually independent and reliable. The background to the sources is important in that regard. The extent to which the data from the source have been verified is also important. Finally the institution verifies the

authenticity of the submitted documents and other sources, considering the risk of forgery and deception attempts.

An institution can also use innovative technologies to organise the customer due diligence or enhanced customer due diligence, as long as the higher risk resulting from the lack of physical presence of the customer is mitigated. To this end the institution can devise new processes for the identification and verification of the customer. These could include, for example, video identification and verification, the reading of the chip on the identity document, the use of a liveness check and the use of an eID device with an appropriate confidence level, or a combination of these. The institution itself determines the exact process on the basis of a risk assessment taking into account the obligations in Sections 3, 5 and 8 of the *Wwft*. Record-keeping and regular review are important in this regard. It should be noted that the use of new technologies is cited as a high-risk factor in Annex III to the fourth Anti-Money Laundering Directive. On 23 January 2018 the European Banking Authority together with the other European Supervisory Authorities (ESMA, EIOPA) issued an opinion on the use of innovations for the customer due diligence.[59] This opinion provides a framework for the use of innovation in the Customer Due Diligence process by institutions.

When using innovative technologies, institutions must in any event take account of the following aspects:

- whether or not firms have appropriate technical skills to oversee the development and proper implementation of innovative solutions, particularly where these solutions are developed or used by a third party (where reliance is placed on such third party in line with Article 25 of Directive (EU) 2015/849) or an external provider;
- whether or not the senior management and the compliance officer have appropriate understanding of the innovative solution; and
- whether or not firms have proper contingency plans in place.

4.9.2 Politically exposed persons (PEPs)

Section 8(5) of the *Wwft* requires institutions to use enhanced customer due diligence for politically exposed persons. The term politically-exposed person (PEP) refers to a person who occupies or has occupied a "prominent public function".[60] Under Section 9a of the *Wwft* the prominent public functions in question are described in Section 2 of the *Wwft* Implementation Decree 2018.[61] The rules on PEPs also apply to direct family members and close associates of a PEP. The Implementation Decree states the functions of the persons so designated. The description of these functions is not exhaustive. The institution must consider the

59 See the 'Opinion on the use of innovative solutions in the customer due diligence process' published on 23 January 2018, available for consultation at: https://esas-joint-committee.europa.eu/Pages/News/ESAS-publish-opinion-on-the-use-of-innovative-solutions-in-the-customer-due-diligence-process.aspx.
60 See the definition of a politically exposed person in Section 1 of the *Wwft*.
61 For the prominent public functions in the Netherlands see the General Guidance on the Anti-Money Laundering and Anti-Terrorist Financing Act (Wwft) of the Ministry of Finance and the Ministry of Justice and Security.

person to be a PEP as long as is necessary. If a PEP ceases to qualify as such, the enhanced customer due diligence must continue for at least a further 12 months. This period is extended as long as necessary until the person no longer represents a heightened risk.

The treatment of PEPs has become more rigorous with the implementation of the fourth Anti-Money Laundering Directive. Domestic PEPs are now also classified as high-risk. The fourth Anti-Money Laundering Directive considers that public functions exercised at sub-national level do not normally need to be considered as exposed persons.[62] However, if their political influence is genuinely comparable to that of similar national positions, institutions are expected to consider designating such persons as high-risk.

Business relations providing services for PEPs require additional measures as they carry higher integrity risks and a higher risk of reputational damage. In addition, the provision of services for PEPs demands special attention as part of the international policy to combat corruption. According to Recital 32 of the fourth Anti-Money Laundering Directive, business relationships with PEPs, particularly individuals from countries where corruption is widespread, may expose the financial sector to significant reputational and/or legal risks. Examples are passive corruption (taking bribes) or misappropriation of public funds. An institution therefore establishes risk-based procedures and measures to identify PEPs and on the basis of Section 8(5) institutions must take appropriate measures to identify the source of the assets and the funds used in the business relationship or the transaction. The fifth paragraph also stipulates that the business relationship will be subject to enhanced monitoring on an ongoing basis.

Institutions carry out assessments on customer acceptance and periodically to determine whether their customer and the UBO qualify as PEPs. This therefore also applies to natural persons who are able to exert material influence or have material interests, or who exert a high degree of influence on the important decisions of an unincorporated partnership or are able to exercise effective control over the policy of an unincorporated partnership. To do so, the *Wwft* requires that institutions have risk-based procedures and measures in place whose depth varies with the customer's or UBO's risk profile.

On the basis of Section 8(5) of the *Wwft* the decision on whether to enter into a business relationship with a PEP or to perform a transaction for a PEP rests with the senior management.[63] The same applies to decisions on whether to continue a relationship with a customer who becomes a PEP. This also applies to UBOs or pseudo-UBOs who quality as PEPs.

62 Article 3(9) of the fourth Anti-Money Laundering Directive states: 'No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials'.

63 Section 1 of the *Wwft*: senior management: a. persons who determine the day-to-day policy of an institution; or b. persons working under the responsibility of an institution who perform a management function immediately below the level of the day-to-day policymakers and who are responsible for natural persons whose activities affect the institution's exposure to the risks of money laundering and terrorist financing. NB: this interpretation of 'senior management' is not the same as the one used in the due diligence concerning the UBO.

How should institutions deal with PEPs?

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

Institutions that have PEPs as customers may also set up their internal procedures for constant monitoring of these business relationships in a risk-based manner. For example, children of a Member of Parliament in the Netherlands with a simple checking account may be less risk-sensitive than the spouse of a head of state of a country with a heightened corruption risk who opens a private banking account. Nevertheless, PEPs essentially represent higher risk.

When conducting customer due diligence in the case of PEPs, the institution will not accept the information submitted by the customer at face value, but where possible will verify it by means of a review and will in any event carry out a credibility check. It may be useful in this regard to be aware of the level of corruption in the country in which the individual fulfils the function, for example by referring to the Corruption Perception Index from Transparency International.[64]

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

Finally, in the case of a person who is no longer a PEP, the institution will use the procedure based on Section 8(7) of the *Wwft* until the person in question no longer carries the higher risk associated with a PEP. That period will be a minimum of 12 months.

Supplementary information

- FATF, Guidance: Politically Exposed Persons (Recommendations 12 and 22), 2013.
- The Wolfsberg Group, Frequently Asked Questions on Politically Exposed Persons, 2008
- Transparency International

64 For more information, see: https://www.transparency.org/research/cpi/overview.

4.9.3 Correspondent relationships

With the implementation of the fourth Anti-Money Laundering Directive, the term 'correspondent bankingrelationship' is replaced by correspondent relationship.[65] It therefore no longer refers only to relationships between banks, but also to relationships between banks and other financial undertakings – such as payment service providers – and relationships among other financial undertakings.

Under Section 8 of the *Wwft*, an institution must conduct enhanced customer due diligence if a correspondent relationship is entered into with an institution established outside the EU. Institutions are expected to obtain a clear picture of other institutions from non-EU Member States with which they enter into correspondent relationships. In correspondent relationships an institution acts in reality as an agent for another bank by effecting payments or performing other services for a customer of the correspondent.

Due to the higher risk involved, the decision on whether to enter into a correspondent relationship rests with senior management under Section 8(4)(c).

It is particularly important to be alert to the potential use of a correspondent account by (unidentified) third parties (transit account or payable-through account), in other words when a customer of the foreign institution has direct access to the account held by that institution at the Dutch institution. The reason why increased attention needs to be paid to this category is that in reality it involves remote service provision.

There may be reasons to conduct enhanced customer due diligence at the start of a correspondent relationship with an institution established in an EU Member State, for example if facts and circumstances point to a higher risk of money laundering or terrorist financing, or if required on the basis of the institution's internal risk classification.

It goes without saying that the obligations in Section 8 of *Wwft* apply in addition to those of Section 3(2) to (4) of the *Wwft*. This means among other things that the obligation to carry out constant monitoring of the business relationship as stated in Section 3(2)(d) of the *Wwft* applies in full to correspondent relationships.

65 The current definition is: correspondent relationship:
a. the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other
liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services; or
b. the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers;

Supplementary information

- The Wolfsberg Group, recommendations for correspondent banking, 2018
- FATF, Guidance on Correspondent Banking, 2016
- Basel Committee on Banking Supervision, Sound Management of risk related to money laundering and financing of terrorism – annex 2 Correspondent banking, 2017

With regard to public sources of information, reference can be made, besides the Internet, to the following documents that have been accepted in an international context:

- The Wolfsberg Group and Bankers Almanac have jointly set up an international database for financial undertakings, the Bankers Almanac Due Diligence Repository.
- Evaluation reports by international organisations such as the FATF, IMF and World Bank. Based on these reports, the institution may request certain information from the other institution, particularly concerning the supervision that is exercised.

4.10 Outsourcing

Under Section 10 of the *Wwft*, the customer due diligence may be outsourced to a third party. With the amendment to the *Wwft* resulting from the implementation of the fourth Anti-Money Laundering Directive, it has been made clear that this provision relates to outsourcing or agency relationships.[66] The provision does not refer to the introduction of customers by other banks or other financial undertakings as referred to in Section 5(1) of the *Wwft*. An institution may outsource customer due diligence to identify the customer, the UBO, a trust or an unincorporated partnership, to verify the identity of those persons and entities and to identify the purpose and envisaged nature of the business relationship. Monitoring of the business relationship may, however, only be carried out by the institution itself.[67]

The institution that has outsourced the due diligence remains responsible for complying with requirements concerning the customer due diligence. In the event of outsourcing to a third party, the institution must therefore prepare a clear risk assessment which includes the expertise and practical approach of the third party in terms of *Wwft* compliance. It is important that institutions not only stipulate in writing that the third party will comply with the *Wwft* and where necessary the institution's policy rules, but that the institution periodically verifies and ascertains this and, if required, reports on it to the third party.

For more information on risks of outsourcing, see the DNB 'Good Practices for control of risks in outsourcing' from 2017.

66 House of Representatives 2017-18, 34 808, no. 3, p. 57.
67 This is because Section 3(2)(d) of the *Wwft* is not referred to in Section 10(1) of the *Wwft*. In the case of institutions governed by the *Wft*, and where the executing party is a member of the same group, such constant monitoring may be carried out by this party within the group.

5 Transaction monitoring and reporting of unusual transactions

5.1 General information

Financial institutions must take measures to prevent money laundering and terrorist financing. To this end they must pay particular attention to unusual transaction patterns and transactions[68] of customers that due to their nature typically carry a higher risk of money laundering or terrorist financing. If there are grounds for assuming that an actual or proposed transaction is linked to money laundering or terrorist financing, they must immediately report it as an unusual transaction to the Financial Intelligence Unit – the Netherlands (FIU - NL). Further information on such reports can be found from Section 5.5 onwards. To be able to do this it is crucial that institutions have in place an effective transaction monitoring process.

The first step in the transaction monitoring process is risk identification. During the identification process institutions systematically analyse the money laundering and terrorist financing risks. The results of this analysis are recorded in the SIRA (see also Chapter 3.2). The SIRA forms the basis for the policy, business processes and procedures relating to transaction monitoring. Institutions must ensure that transaction monitoring process reflects the risks identified in the SIRA. The transaction monitoring process is also based on risk.

When identifying and analysing risks, institutions should place their customers in various risk categories – such as high, medium and low – based on the risks pertaining to the business relationship with the customer (see also Chapter 3.4).

To determine a customer's risk profile, institutions prepare a transaction profile based on the expected transactions or the expected use of the customer's (or customer group's) account. By preparing a transaction profile in this way institutions can sufficiently monitor transactions conducted throughout the relationship to ensure they are consistent with the knowledge they have of the customers and their risk profile. By identifying the expected transaction behaviour, institutions can assess whether the transactions conducted are consistent with their knowledge of the customer. Customers' transaction profiles may be drawn up on the basis of 'peer grouping'. It is important throughout the relationship that the institution checks periodically whether the customer still matches the risk profile and whether the transaction pattern is in line with expectations.
The institution may tailor the frequency and intensity of reviews to the customer's risk classification.

The monitoring of the relationship with the customer and the transactions may be geared to the type of relationship with the customer and the risk profile. This may vary depending on the sector and product. For instance, for life insurance products, annual checks could be conducted, e.g. when annual and other premiums are paid, and also when the contract or the beneficiary changes. If the policy leads to a long-term relationship with the beneficiary (e.g. in the case of annuity payments), continual monitoring of the payouts has no added value, as these payments are made by the institution itself.

68 A transaction is defined as: An action or series of actions by or on behalf of a customer of which the institution has become aware in providing its services for that customer.

Good Practices in transaction monitoring

DNB provides guidance on how institutions can establish and improve the transaction monitoring process. In preparing these Good Practices, DNB has drawn on the main findings from the 2016 thematic examination: "Post-event transaction monitoring".

The key features of an appropriate transaction monitoring system are as follows:

1. Institutions must ensure that the transaction monitoring process reflects the risks of money laundering and terrorist financing that emerge from the SIRA. When determining the risk profile for a customer and/or 'customer peer groups', institutions must also take account of the expected transaction behaviour.
2. Institutions must have developed an adequate policy for transaction monitoring and have sufficiently elaborated this policy in underlying procedures and operating processes.
3. Institutions must have an automated transaction monitoring system in place and have a substantiated and adequate set of business rules (detection rules with scenarios and threshold values) to detect money laundering and terrorist financing. Institutions must periodically test these business rules, in terms of both technical aspects and effectiveness.
4. Institutions must have an adequate process for notification and dealing with alerts. Institutions must ensure that they fully and immediately notify FIU-NL of any intended or executed unusual transactions. As part of this process, a record is made of the considerations and conclusions underlying decisions to close or escalate an alert.
5. Institutions must have structured their governance with regard to transaction monitoring in such a way that there is clear segregation of duties, for example through the three lines of defence model.
6. Institutions must offer their staff tailored training programmes. Staff are aware of the risks of money laundering and terrorist financing.

In addition to the key features, the Good Practices below include sector-specific examples.

- Banks
- Payment service providers
- Money transfers
- Trust offices

For examples of tax integrity risks see the Good Practices for tax integrity risks of banks and trust offices (Chapter 6).

5.2 Recognising patterns and transactions

Institutions analyse their transaction data with the aid of the transaction monitoring system and software. The system generates alerts based on business rules. An alert is a signal that indicates a potentially unusual transaction. These alerts are investigated. The findings of the investigation into the alerts must be adequately and clearly recorded. If the investigation reveals that a transaction can be earmarked as unusual, the institution must report it to FIU-NL without delay. It must clearly explain and document its considerations and decision-making process regarding whether or not to report a transaction. If in doubt as to whether a transaction is unusual, the institution should always report it to FIU-NL. Failure by an institution to fulfil its reporting duty or to do so on time – even unintentionally – constitutes an economic offence.

Before carrying out transaction monitoring, institutions guarantee that all data will be fully and accurately included in the transaction monitoring process. For example, this may be data concerning the customer, the services and the transactions. The term 'transaction' is construed broadly in the *Wwft* and described as an 'action or series of actions by or on behalf of a customer…'. This means that all information associated with the financial transaction data which becomes known to the institution in the provision of the services can be included. If there are large numbers of transactions, it is appropriate to have an automated transaction monitoring system in place to guarantee the effectiveness, consistency and processing time of the monitoring.

The system must at least include predefined business rules: detection rules in the form of scenarios and threshold values. In addition, more advanced systems may also be desirable, and necessary in certain cases, depending on the nature and the size of the transactions and the nature of the institution in question. For example, a smaller institution with a limited number of simple transactions would have less need for a highly advanced system. An institution may also deem it necessary to use highly advanced systems, for example with artificial intelligence. The use of advanced systems assumes that the institution itself possesses sufficient knowledge to establish and use these types of systems. The quality and effectiveness of the system must be demonstrable. An institution can adequately assess the quality and effectiveness of its transaction monitoring by arranging a model validation or audit.

The institution remains responsible in any event for the effective detection of unusual transactions. An institution must have a good understanding of the systems and cannot therefore rely on algorithms provided by external suppliers.

Key points in transaction monitoring

- Do the transactions serve an economic or commercial purpose?
- Do the transactions involve exceptionally large amounts?
- Do the transactions involve deposits, withdrawals or transfers that are not consistent with the customer's normal or expected business?
- Are the account and transaction movements consistent with the customer's activities?
- Are there any transactions to and from high-risk countries?
- Does the structuring of transactions entail any tax integrity risks?

5.3 Focus on high-risk jurisdictions

The FATF regularly identifies jurisdictions that have deficiencies in their anti-money laundering and anti-terrorist financing systems. Maintaining business relationships with residents of such jurisdictions, or effecting transactions to or from these jurisdictions, may entail an increased risk of money laundering and terrorist financing, which could lead to enhanced transaction monitoring. The FATF updates the lists, where appropriate, and DNB refers to them on its website.

The European Commission also identifies third countries that have deficiencies in their anti-money laundering and anti-terrorist financing systems.[69] Institutions take account of these high-risk countries in their transaction monitoring.

In addition to the warnings from the European Commission, the FATF and FATF Associate Members,[70] there are other reliable sources indicating the extent to which a country or jurisdiction implements international standards in the combating of financial crime or terrorist activities. These sources may also prompt an institution to devote greater attention to business relationships and transactions involving people from those countries and jurisdictions. Institutions take the risks of money laundering and terrorist financing in specific countries into account as part of their monitoring.

5.4 Assessment of transactions, measures and reporting

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

69 Under Section 9 of the fourth Anti-Money Laundering Directive (2015/849) the European Commission identifies third countries with deficiencies in combating money laundering and terrorist financing.

70 FATF Associate Members are: Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Eurasian Group (EAG), Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering measures and the Financing of Terrorism (MONEYVAL), Financial Action Task Force of Latin America (GAFILAT), Inter Governmental Action Group against Money Laundering in West Africa (GIABA) and the Middle East and North Africa Financial Action Task Force (MENAFATF).

or terrorist financing and must record its findings in the customer file. If a transaction is suspected of being linked to money laundering or terrorist financing, it must be reported to FIU-NL without delay in accordance with Section 16 of the *Wwft*. Institutions must document their considerations and decision-making process regarding whether or not to report a transaction.

They must assesses the consequences of the report to FIU-NL and any feedback report from FIU-NL for the customer's risk profile and determine whether any additional control measures need to be taken. The final part of the transaction monitoring process is the retention of the data obtained from transaction monitoring. In this connection, the institution must retain the data relating to the report of the unusual transaction and record it in readily accessible form for five years after the report was made, allowing the transaction to be reconstructed.

The Good Practices for transaction monitoring include a maturity model describing all stages of the transaction monitoring process together with the associated conditions for efficient organisation.

5.5 Obligation to report unusual transactions

Section 16 of the *Wwft* requires institutions to report executed or proposed unusual transactions. The annex to Article 4 of the *Wwft* Implementation Decree 2018 lists the indicators on which reports must be submitted. This list can be used to assess whether transactions should be earmarked as unusual. The indicators are divided into objective indicators and the subjective indicator. The objective indicators describe situations in which transactions must always be reported. The Annex to the Implementation Decree[71] makes clear which objective indicators apply to which institutions. For example, the money transfer indicator applies to banks, electronic money institutions, financial institutions, payment service agents and payment service providers.

However, the emphasis in the reporting obligation is on the subjective indicator. The subjective indicator requires an institution to report a transaction if it has reason to suspect that the transaction may be related to money laundering or terrorist financing. This indicator applies to every institution that falls within the scope of the *Wwft*. The institution must therefore assess whether a particular transaction should be reported because of a possible link to money laundering or terrorist financing. The institution thus has its own responsibility for the adequate reporting of unusual transactions.

71 The *Wwft* Implementation Decree 2018 is available for consultation at: https://wetten.overheid.nl/BWBR0041193/.

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

The definition of a transaction[72] is intended to make clear that an unusual transaction by the customer or by a third party acting on behalf of the customer must always be reported if the institution has become aware of it in the course of providing services for that customer. It is not a requirement that there must be a direct or causal connection between the unusual transaction and the activities of the institution. The words "action or series of actions by or on behalf of a customer" should be interpreted in such a way that the passive involvement of the institution (by virtue of its knowledge of the transaction) can also trigger the statutory reporting obligation.

5.5.1 Life insurers' reporting obligation

Life insurance products are generally products with lower money laundering and terrorist financing risk. Despite the lower risk, it is still possible that products will be purchased with the proceeds of financial and economic crime. There is also a risk that assets may be withdrawn to finance terrorism. On 25 October 2018 the FATF issued the 'Risk-based Approach Guidance for the Life Insurance Sector'.[73] This document provides guidance for life insurers on the adoption of a risk-based approach.

The examples below concern indicators of transactions in which the life insurer has grounds to investigate the transaction further and to assess whether there are any factors requiring the transaction to be designated as unusual. The file handler will notice some of those transactions in the initial work process. For some of the other indicators the life insurer will perform regular queries to assess whether transactions may have been unusual.

72 Transaction: an action or series of actions by or on behalf of a customer of which the institution has become aware in providing its services for that customer, Section 1 of the *Wwft*.

73 The FATF 'Risk-based Approach Guidance for the Life Insurance Sector' is available for consultation at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-life-insurance.html.

Examples of indicators of possible unusual transactions for life insurers.

- High single premium or high additional premiums paid into the policy.
- Premium payments from a country designated as high-risk.
- Policyholder, beneficiary or premium payer residing in the Netherlands moves to a country designated as a high-risk.
- Surrendered (single or regular premium) policies running for less than three years with a surrender value of [€ xx] or more and a surrender value amounting to 50% or more of the total paid premiums.
- Policyholder, beneficiary or premium payer is a foreign legal entity or a natural person resident or established outside the Netherlands.
- Annual payments totalling over [€ xx] to high-risk countries.
- One-off payouts of [€ xx] or more.
- Annual periodic payouts of [€ xx] or more.
- Premium payback on single premium policy (other than assured premium repayment) of [€ xx] or more.
- Policies cancelled inside the 30-day statutory cancellation period and involving a premium payment/repayment of [€ xx] or more.
- Pledging or collateralisation of the policy for an amount of [€ xx] or more, for a purpose other than mortgage lending.

More examples

FATF, 'Risk-based Approach Guidance for the Life Insurance Sector', 2018

5.5.2 Reporting obligation for credit cards

The 'red flags' set out below can provide support in detecting unusual credit card transactions.

Examples of indicators of possible unusual transactions in the case of credit card transactions

Funding of the card

1. Cash payments into a checking account, the purpose of which is to pay for credit card expenditure.
2. Funding by a third party (other than the cardholder) and from another country.

Use of the card

- Excessive ATM use or reverse transfers to another account by natural persons without a clear rationale
- Excessive purchasing of other card or stored-value (voucher) products
- Frequent and substantial transactions at casinos
- Frequent and/or substantial transactions with not-for-profit organisations (donations)
- (Presumed) delivery of intangible goods or services
- Concentration of frequent high-value transactions by a small group of cardholders with particular merchants (purchase of luxury products)
- Structured use of stolen credit cards at e-commerce merchants

Other signals

- Problems with identification and/or verification (applicant and/or UBO)
- Dependence of merchant on certain cardholders due to turnover (volume)
- Relationships between cardholder(s) and merchant(s) (criminal organisation and anonymous use)
- Forgery
- Cybercrime (including phishing, skimming and use of malware)

5.6 FIU reporting procedure

An inherent part of the reporting duty under Section 16 of the *Wwft* is that institutions have in place processes and procedures to recognise and report the unusual nature of transactions. Executed or proposed unusual transactions must be reported to FIU-NL without delay as soon as their unusual nature becomes known. Furthermore, as also stated in the annex to the *Wwft* Implementation Decree 2018, where transactions are reported to the police or the Public Prosecution Department in connection with suspected money laundering or terrorist financing, they should also be reported to FIU-NL due to the suspicion of money laundering or terrorist financing.

The *Wwft* lists the data to be submitted when reporting an unusual transaction. These data are vital for FIU-NL to be able to analyse an unusual

transaction. If an institution systematically fails to submit specific data, FIU-NL can report this omission to the supervisory authority, which in turn can issue an official instruction to the institution to develop internal procedures and controls for the prevention of money laundering and terrorist financing.

FIU reporting procedure

Institutions that are subject to the reporting requirement contact FIU-the Netherlands to gain access to the reporting portal. More information can be found on the FIU website.

5.7 Indemnification

Section 19 of the *Wwft* provides for criminal indemnification and Section 20 for civil indemnification. Criminal indemnification ensures that data or information provided by an institution that reports an unusual transaction in good faith cannot be used in a criminal investigation or prosecution of that institution on suspicion of money laundering or terrorist financing. The Act extends this indemnification to those who have submitted the report, such as a bank employee who submitted or helped compile the report.

Civil indemnification means that an institution cannot be held liable under civil law for the loss suffered by another party (e.g. the customer or a third party) as a result of a report as long as the institution acted on the reasonable assumption that it had fulfilled its reporting duty. For instance, claims in civil proceedings could be brought for breach of contract if the institution decided not to carry out a transaction but to report it. Legal action over an unlawful act is also possible, if a customer claims alleged loss suffered as a result of an institution's unusual transaction report.

The indemnification will of course only apply if the unusual transaction report has been submitted correctly, in good faith and in accordance with the requirements of the *Wwft*.

5.8 Confidentiality under the Wwft

Section 23 of the *Wwft* imposes a duty of confidentiality on institutions. They are obliged among other things not to disclose that a report has been submitted under Section 16 of the *Wwft*. Exceptions are possible to the extent that the law permits. Put briefly, the exceptions to the confidentiality obligation allow the institution to exchange information with units of its own organisation or network elsewhere and/or with other institutions that fall within the scope of the *Wwft* or equivalent legislation, within the framework of the said laws. Without these exceptions, existing early-warning systems between financial institutions, such as the interbank warning system, could be obstructed.

On the basis of Section 23a of the *Wwft*, institutions are obliged to share reports under Section 16 of the *Wwft* within the group unless the FIU specifies otherwise.

5.9 Legal claims and confidentiality under the Wwft

Institutions may face demands from the Public Prosecution Department to supply customer information as part of a criminal investigation into a customer (or into third parties). The institution is subject to a confidentiality obligation.

A demand may be grounds for the institution to conduct more detailed and possibly enhanced customer due diligence and to carry out additional monitoring of the customer's transactions. The results of the more detailed customer due diligence may be grounds for institutions to take control measures or report unusual transactions to the FIU without discussing the demand with the customer. If the Public Prosecution Department does not want the customer to know that an investigation is ongoing, this will be explicitly stated in the demand. This means that if the institution takes control measures, the customer must not be aware of them.

A demand from the Public Prosecution Department does not necessarily require an institution to terminate the customer relationship on the basis of the *Wwft* or the *Wft* or to suspend services. An institution may conclude on the basis of its customer due diligence that the risks posed by the customer are unacceptable and that there are grounds for terminating the relationship. If there are indeed unacceptable risks or if it is not possible to meet the customer due diligence requirements, the institution may terminate the customer relationship at the first opportunity.

However, if the criminal investigation requires the customer relationship and the transactions to be continued, this possibility will no longer be available. The request to continue the customer relationship and the transactions will be stated in the demand by the public prosecutor.

In that situation enhanced monitoring of the customer and his transactions and careful recording of the relevant facts and circumstances in the customer file can provide the necessary safeguards to address the risks. Institutions may only terminate a relationship with a customer on the basis of the demand if the Public Prosecution Department gives its consent.

Finally, in the above situations the obligation to report unusual transactions effected by or on behalf of persons to whom the demand relates remains fully in force.

6 The Regulation on information accompanying transfers of funds (Wire Transfer Regulation 2)

6.1 General information

The EU regulation on information accompanying transfers of funds, also known as the Wire Transfer Regulation 2 (WTR2), contains provisions on the traceability of transfers of funds to prevent, detect and investigate money laundering and terrorist financing. The regulation requires institutions to supply information with transfers of funds and to carry out checks of incoming transfers so that information on the payer and the beneficiary remains traceable in the payment chain. In its supervision of financial institutions, DNB monitors these institutions' compliance with the obligations ensuing, inter alia, from the *Wwft*.[74]

6.2 Background to WTR2

Regulation (EU) 2015/847 on information accompanying transfers of funds came into force on 26 June 2017. This Regulation succeeded and repealed the Wire Transfer Regulation (WTR1, EC Regulation no. 1781/2006). The purpose of the WTR1 and WTR2 Regulations is to improve the traceability of information accompanying transfers of funds in order to contribute to the prevention, detection and investigation of money laundering and terrorist financing.

WTR1 contained obligations regarding the recording of information on the payer in transfers of funds. WTR2 expands the obligations with regard to the recording of information accompanying transfers of funds. The key requirement is that in addition to information on the payer, information on the beneficiary must also be recorded. This page provides a brief summary of WTR2.

6.3 Scope of application

WTR2 applies to transfers of funds sent or received by a payment service provider or an intermediary payment service provider established in the European Union (Article 2). The scope of application is broad, but there are a number of exceptions (Article 2 of WTR2), e.g. for credit and debit cards, electronic money transfers and transfers effected with a mobile phone or other digital or IT device.

6.4 Obligations of payment service providers and intermediary payment service providers

Chapter II of WTR2 is divided into two sections, with one section addressing the obligations of the payment service provider of the payer and the other addressing the obligations of the payment service provider of the payee. Briefly, the payment service provider of the payer is responsible for adequate recording of information, while the payment service provider of the payee must check whether the information received is complete. Article 4 of WTR2 describes which information must be recorded and sent with the transfer of funds. This depends on whether the transfer of funds takes place within the

74 Section 1d(2) of the *Wwft*.

European Union, from outside the EU to within the EU or from within the EU to outside the EU (Section 5 and 6 of WTR2). The intermediary payment service provider must ensure that all information concerning the payer and the payee is retained and included with the transfer.

6.5 Detecting and assessing incomplete information

The payment service provider of the payee must have procedures in place to examine and assess whether the information sent is complete (Article 8). These procedures must be conducted on a risk basis. If the information is found to be incomplete, the transfer of funds must be suspended or rejected, depending on which information is missing. Intermediary payment service providers are subject to specific rules (Articles 10, 11 and 12 of WTR2), depending on whether the transfer is effected within, from or to the European Union. The European Banking Authority (EBA) has issued Guidelines on this topic.

6.6 EBA Guidelines

On 22 September 2017, the European supervisory authorities (EBA, EIOPA and ESMA) issued Joint Guidelines on WTR2. The document provides guidelines on the procedures that financial undertakings must have in place to deal with missing information on the payer or the payee in transfers of funds. [75]

6.7 FIU notifications

If information on the payer or payee is missing, this may be a reason to notify the Financial Intelligence Unit (FIU) of an unusual transaction. This applies to both payment service providers and intermediary payment service providers (Articles 9 and 13 of WTR2). The Joint Guidelines list a number of additional factors that may be relevant here, such as transfers to and from high-risk countries, transfers exceeding a specific value threshold or transfers where the name of the payer or payee is missing. See item 30 of the Joint Guidelines for more information.

6.8 Integrity supervision under the Wwft

The WTR2 obligations must be seen in the light of the applicable obligations with regard to the *Wwft*. Financial institutions must integrate the WTR2 obligations into their operational procedures.

Joint Guidelines – Wire Transfer Regulation 2

For further details of the Regulation see 'the Joint Guidelines' of the European Supervisory Authorities (EBA, ESMA and EIOPA).

75 Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information.

7 Sanctions regulations

7.1 General information

The Guidance issued by the Ministry of Finance provides extensive information on sanctions. In addition, a description is given below of DNB's supervision of compliance with the Sanctions Act 1997 (Sw) and the accompanying reporting procedure.

The AFM and DNB have been entrusted with the supervision of compliance with the Sw with regard to financial transactions. To that end, the two supervisory authorities jointly adopted the Regulation on Supervision pursuant to the Sanctions Act 1977 (Regeling Toezicht Sanctiewet 1977). This Regulation states that an institution must take measures to verify whether customers of the institution appear on one or more sanctions lists (such as EU decisions and/or Regulations, decisions of the Dutch Minister of Foreign Affairs based on the Dutch regulation on terrorism sanctions 'Sanctieregeling Terrorisme 2007-II' – also referred to as the 'Dutch List'[76]– or UN Security Council Resolutions). The European Union Regulations and national sanctions regulations describe several financial sanctions:

- orders to freeze financial assets of designated individuals and organisations
- a ban on making resources available to these individuals or organisations directly or indirectly
- a ban or restrictions on providing financial services (for persons, entities or goods)

An institution is expected to make its own risk assessment as a basis for measures to implement the sanctions regulations. This requires an appropriate risk analysis by the organisation, which can be developed within the SIRA system (see Chapter 3.2).

An institution must at all times be able to detect whether any of its customers are named in or its services and transactions relate to the sanctions regulations. An institution must also notify, or be able to notify, DNB of such cases without delay under Article 3 of the Regulation on Supervision under the Sanctions Act 1977. This requirement cannot be fulfilled on a risk basis, so the institution cannot opt to not comply with the sanctions regulations and dispense with the continuous screening of customers.

An effective screening process enables an institution to comply with sanctions regulations and is characterised by frequent screening. The screening times must be set in such a way that institutions are at all times in a position to find out whether their customers appear in or their services and transactions relate to the sanction regulations. The risk of violations of sanctions regulations can be reduced by screening at the time of acceptance, when relevant changes occur in the customer's position, when changes are made to the sanctions list and when transactions are effected.

76 For the Dutch sanctions list of individuals and organisations with frozen assets, https://www.rijksoverheid.nl/onderwerpen/internationale-sancties/documenten/rapporten/2015/08/27/nationale-terrorismelijst.

Important screening times

- acceptance
- relevant changes in the customer's position
- changes in the sanctions lists transactions

7.2 Administrative organisation and internal control (AO/IC)

In its capacity as the supervisory authority, DNB assesses and enforces the effectiveness of the procedures and measures undertaken by institutions aimed at compliance with sanctions laws. In practical terms, when taking measures, an institution may seek alignment with existing administrative organisation and internal control (AO/IC) rules that arise from other regulations such as the *Wft* and the *Wwft*. The basic principle for the implementation of the AO/IC by the financial institution is that it should act in accordance with the objectives of the sanctions regulations. Briefly, this means that institutions are able to check their records in such a way that business relations, goods and transactions that are subject to sanctions can be identified. It must be possible to freeze the financial assets immediately and/or to prevent financial assets and/or services being made available. No relationship with an existing customer must be terminated and in some cases dispensation may be sought from the Ministry of Finance. If the institution finds that the identity of a business relation matches that of an individual, legal person or entity referred to in the sanctions regulations (a so-called hit[77]), it must notify DNB immediately. The way in which hits must be reported to DNB is further explained in section 8.5.

In its assessment of the AO/IC, DNB looks, for example, at the following elements:

- The sanction risks that the institution incurs as recorded in the SIRA
- The design of the sanctions policy, the procedures and the codes of conduct
- The application of the institution's own sanctions policy in the customer files
- The screening process (including the handling and recording of hits)

Training and awareness

77 An institution will encounter many potential hits when screening against the sanctions lists. These are all checked for correspondence with the various lists. Only genuine hits are reported. False positives are not reported.

7.3 The 'relationship' concept

The 'relationship' concept

The Regulations adopt a broad definition of the term 'relationship' covering any party that is involved in a financial service or financial transaction. This includes:

- customers
- representatives or authorised agents
- UBOs of the customers
- beneficiaries of a product (e.g. life insurance payments) or domestic or international transfers of funds
- counterparty to a financial transaction/ product (e.g. non-life insurance payments)
- person(s) involved in a financial transaction to which a company receiving services from a trust office is party
- directors of customers and parties related to customers

The term 'relationship' is defined so broadly because both the direct and indirect provision of financial resources or services falls under the sanction measures. In April 2013 new elements were added to the "Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy". These new elements state that the making available of funds to persons or entities that do not appear on the sanctions lists but are controlled or owned by persons or entities that do appear on the sanctions lists is in principle deemed to constitute the indirect making available of funds to the sanctioned person or entity.[78]

Financial resources or services are made available indirectly if a person holds 50% or more of the ownership rights in a structure or if a person (for example a director) has control (which term is defined very broadly in the Guidelines). If the person holding 50% or more of the ownership rights or having control of an entity appears in a sanctions list, the assets of that entity must also be frozen and no funds must be released to it. In practice, institutions may also identify UBOs in the case of ownership percentages below 50%. It is therefore recommended that institutions apply the definition of UBO set out in the *Wwft* and therefore ascertain the identity of all UBOs holding 25% or more of the ownership rights, as institutions are prohibited from making assets available to persons or entities under the control of a sanctioned person. Control of an entity does not require ownership of 50% or more of the shares. There is a risk that UBOs will have control through various entities within a structure.

In the case of customers that are only partly listed on a stock exchange, it is important with regard to compliance with the sanctions regulations that the UBO of the unlisted part is known.

During the customer acceptance process, all relationships are defined and recorded in the relationship file. As well as the customer, this also

78 Guidelines on implementation and evaluation of restrictive measures (sanctions). Available for consultation at: https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf.

includes other persons and entities involved in the financial service or transaction, such as the customer's UBO(s), representatives, directors, authorised agents and beneficiaries (where known). Since the term 'relationship' is defined so broadly, an institution surveying all relationships must assess the extent to which a particular relation has or can have ownership or control of the funds.

During the identification process, information is recorded such as the name, date of birth, place of residence and registered address of these persons and entities. This information enables the institution to perform proper checks. The absence of a date of birth or place of residence, for example, can make it more difficult to assess a hit. In the case of legal persons, it is generally sufficient to check the information contained in the Trade Register at the Chamber of Commerce, while for natural persons a check of a passport or a copy of the passport is generally sufficient to enable adequate screening against the sanction regulations.

In the case of relevant changes in the customer's position, for example a change in relationships or UBOs, an institution must update its customer database. In the case of relationships that qualify as high-risk (for example customers trading with sanctioned countries), an institution is expected to play a more active role in identifying changes. That can be done, for example, by conducting periodic enquiries to identify any changes in the relevant relationships. The full customer database can then be included in the screening process.

The institution must also investigate whether a ban or restriction applies to the financial service or transaction in relation to certain countries and regions and/or certain goods (embargoes). The institution must record this information in an accessible way.

Focus on strategic goods and proliferation

Some sanctions regimes include bans or restrictions on providing financial services for goods. These include, for example, military goods, 'dual-use' goods, strategic services (e.g. software and technology) and goods that can be used for internal repression (torture goods).

More information on these goods (available in Dutch only).

7.4 Transaction monitoring

The principle is that the parties involved in transactions (relations) are screened against the sanctions lists. The institution must ensure that its AO/IC is configured in such a way that sanctions regulations are complied with even in the case of payments effected with the assistance of third parties. If sufficient agreements have been made with the third parties on compliance with the sanctions regulations, the institution can have confidence that the third parties will freeze assets if necessary. The agreements should include provisions whereby institutions inform each other

of transactions that will be frozen and foreign third parties will also use Dutch sanctions lists during the screening process. The institution must ensure that its AO/IC is configured in such a way that the objectives of the sanctions regulations are complied with even in the case of payments to third parties.

How does an institution filter transactions against sanctions lists?

Information or fields against which checks are carried out as a minimum:

- payer
- payee
- place names
- country
- description

Institutions conducting payments filter the SWIFT MT series and fields (including n99 messages) and SEPA messages and fields that the institution has identified on the basis of a documented risk assessment.

Trust offices, insurers and institutions with limited payment transactions carry out checks when making payments to beneficiaries as to whether the natural or legal person concerned appears on the sanctions lists.

7.5 Reporting to DNB

In the event of a hit, the institution reports the following to the supervisory authority:

- identifying data (name, alias, address, place and date of birth)
- the nature and size of the frozen deposits or assets
- the action taken by the institution
- the applicable sanctions regulation(s)

Institutions send hits to DNB using the report format drawn up by the AFM and DNB.[79] DNB assesses the completeness of the reports received from financial institutions. Institutions report the cases in which there is an actual hit. If an institution doubts whether a hit report represents a genuine hit, it must conduct further research to confirm or rule out a match with the sanctions lists.

Exemptions are possible in some cases (this may vary depending on the sanctions regulation). The Minister of Finance is authorised to decide on this. A substantiated request for exemption can be sent to the Ministry.

79 See also the DNB website: https://www.dnb.nl/en/sector-information/supervision-laws-and-regulations/laws-and-eu-regulations/sanctions-act-1977/getting-around-in-sanctions-regulations/

Example of a grant of exemption

This concerns the special case of liability insurance For example, a customer of an insurer who has taken out third-party liability insurance causes a collision. On settlement of the claim, the insurer has to pay damages to the victim/beneficiary. However, upon checking it transpires that the beneficiary appears on the sanctions lists, so the insurer is required to freeze the funds under the sanction regulations, whereas under other regulations it may have an obligation to pay out. In such cases, the institution freezes the funds and uses the report format to notify DNB, which then forwards the report to the Minister of Finance. On the basis of a substantiated exemption request, the Minister can then decide whether an exemption can be granted. In the case of other insurance policies where the beneficiary is unknown, the insurer must also check whether the sanction regulations apply when a claim is submitted.

7.6 Hit reports, FIU reports and deadlines

When institutions freeze assets on the basis of a hit on sanctions lists, they are also expected to look at the transaction history to see whether any transactions have taken place that could be assumed to be related to money laundering or terrorist financing. If money laundering or terrorist financing is suspected, institutions must report this to the FIU under Section 16 of the *Wwft*.

Assets must remain frozen until the relevant sanctions regulation is amended and the obligation to freeze the assets is lifted, an exemption is granted or notice to the contrary is received from the Minister of Finance or DNB. If the institution does not hear anything, it must assume that the assets are to be considered an actual hit and must remain frozen until further notice.

The reported data must be retained for a period of five years after the relevant sanctions regulation has ceased to have effect or has been rendered inoperative.

Supplementary information
Dutch government – International sanctions

http://www.rijksoverheid.nl/onderwerpen/internationale-sancties

Ministry of Foreign Affairs – Sanctions summary page – Restrictive EU measures
https://ecer.minbuza.nl/ecer/dossiers/buitenlands-en-veiligheidsbeleid/sancties.html

DNB – Sanctions Act 1977
https://www.dnb.nl/en/sector-information/supervision-laws-and-regulations/laws-and-eu-regulations/sanctions-act-1977/

DNB – Q&A on the Sanctions Act for non-life insurance companies
https://www.dnb.nl/media/ua5dp5p1/q-a-sanctiewet-voor-schadeverzekeraars.pdf (available in Dutch only).

DNB – Guideline on the Sanctions Act for Pension Funds
https://www.dnb.nl/media/g23b1w3t/naleving-sanctiewet-voor-pensioenfondsen.pdf (available in Dutch only).

8 Record-keeping, data retention obligation and the General Data Protection Regulation (GDPR)

Various laws[80] stipulate that institutions must retain customer and transaction data. This concerns all data obtained during the CDD process, e.g. copies of identity documents, account information, correspondence, memos of conversations about and with the customer, transactions effected by the customer and other services provided for the customer. The customer file must also show how the decision-making process surrounding customer acceptance has taken place, e.g. in the case of high-risk customers.

For legal entities, records must include the particulars of the natural persons representing the legal entity vis-à-vis the institution. For the UBO, the person's identity and the method by which it was verified must be recorded. Where a customer acts as a trustee, the institution must also record, in a retrievable way, the particulars of the settlors, the trustees and the UBOs. If the customer acts as a partner in an unincorporated partnership, the institution records the details of the partners, the persons authorised to manage the partnership and the persons who are able to exert considerable influence on or have considerable interests in the partnership.

The purpose of the data retention obligation is, inter alia, to enable the authorities to understand a customer's activities, e.g. in the event of an examination or criminal investigation. The various records and files must therefore be readily accessible to the supervisory authority. It makes no difference whether the data are stored electronically or as a physical document.

The Guidelines entitled 'Identification and verification of personal data' issued by the College Bescherming Persoonsgegevens, the predecessor of the current Dutch Data Protection Authority, state that a financial institution can also retain a copy of the inspected identity document – as proof of the identification obligation (reconstruction obligation). Under Section 33 of the *Wwft* there is no obligation to record the Citizen Service Number (BSN).[81]

The current *Wwft* takes account of the General Data Protection Regulation (GDPR). A key principle of the GDPR is 'purpose limitation', which is detailed in Section 34a(1) of the *Wwft*. Personal data collected under the *Wwft* can in principle only be processed for the purpose for which it was initially collected, namely compliance with the *Wwft* with a view to preventing money laundering and terrorist financing.

In addition to the purpose limitation, Section 34a(2) of the *Wwft* states that institutions must inform customers of the legal obligation covering the processing of personal data under the *Wwft*. This could include informing customers about the purpose of the processing of the data and the statutory retention period that applies in respect of such data.

80 Sections 33, 34 and 34a of the *Wwft*, Article 14 of the Prudential Rules (Financial Supervision Act) Decree, Article 10, of Book 2 of the Dutch Civil Code, Section 52 of the State Taxes Act.
81 Available for consultation at: https://wetten.overheid.nl/BWBR0033181/

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl