DNB Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act and the Sanctions Act

Preventing the misuse of the financial system for money laundering and terrorist financing purposes and controlling integrity risks

Version 3.0 – April 2015

Contents

1. INTRODUCTION

1.1 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 Counter-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme* / Wwft), the Trust Offices Supervision Act (*Wet toezicht trustkantoren* / Wtt) and the Sanctions Act 1977 (*Sanctiewet 1977* / SW).

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 the implementation of the Wwft has been assigned to DNB for the following types of institutions: banks, life insurers, payment services providers and agents, electronic money institutions, foreign exchange offices, trust offices, lease companies and casinos (Holland Casino). In addition to these institutions, for the purposes of the Sanctions Act, pension funds and other insurers are also subject to DNB supervision.

DNB assesses and enforces the adequacy and effectiveness of the procedures and measures implemented by supervised institutions to combat money laundering and terrorist financing. Enforcement takes place in conformity with the Enforcement Policy of the Netherlands Authority for the Financial Markets (*Autoriteit Financiële Markten* / AFM) and DNB on the basis of standards laid down in legislation and regulations.

A first Guidance was drawn up by DNB in 2011 on the recommendation of the Financial Action Task Force (FATF). This Guidance provided institutions supervised by DNB with tools to enable them to comply with the statutory obligations arising from the integrity regulations. This third edition of the Guidance incorporates a number of changes in the light of relevant amendments to the Wwft, which came into effect on 1 January 2015 (Bulletin of Acts and Decrees (*Staatsblad*) 2014, no. 472) and the entry into effect of the Regulation on sound operational management under the Wtt 2014 (*Regeling integere bedrijfsvoering Wtt 2014* / Rib Wtt 2014) (Government Gazette (*Staatscourant*) 2014, 20684).

In addition to incorporating relevant legislative changes, new good practices have been added on some points, which have emerged from DNB's supervision investigations in the past year.

Chapters 2 and 3 address the overall regulatory framework on integrity issues that is relevant for all institutions, as well as the integrity risk analysis and the integrity policy. Chapters 4 through 8 concern the requirements of the Wwft and Wtt relating to topics as client examination, monitoring and the reporting duty. [1] Chapter 9 addresses the sanctions regulation and in chapter 10 guidance is provided on training and education.

In this document, purple blocks contain recommendations, good practices and red flags. The green blocks contain references to other relevant documents that institutions can use when devising their integrity policy. Finally, the orange blocks contain information relating specifically to trust offices.

1.2 Purpose and status of the DNB Guidance

This Guidance is not a legally binding document or a DNB policy rule as referred to in Section 1:3(4) of the General Administrative Law Act (*Algemene Wet Bestuursrecht*), and it does not have or aim to have any legal effect. This Guidance does not replace laws and regulations or policy and supervisory rules on the issues concerned, such as the Regulation on Protected Accounts under the Financial Supervision Act (*Regeling afgeschermde rekeningen Wft*) or the Policy Rule on Integrity Policy regarding Commercial Real Estate Activities (*Beleidsregel Integriteitbeleid ten aanzien van zakelijke vastgoedactiviteiten*). The examples presented in this Guidance are not exhaustive and cannot cover every eventuality. They serve as a guide for the explanation and application of statutory obligations.

This DNB Guidance applies to institutions that are subject to DNB supervision, and complements the 'General Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act (Wwft) and the Sanctions Act (SW)' by the Dutch Ministry of Finance. [2] Both guidance documents clarify

[1] Chapters 4 through 8 are not applicable to non-life insurers as these institutions are not subject to the Wwft.
[2] http://www.rijksoverheid.nl/ministeries/fin/documenten-en-publicaties/richtlijnen/2011/02/21/algemene-leidraad-wet-ter-voorkoming-van-witwassen-en-financieren-van-terrorisme-wwft-en-sanctiewet-sw.html

the various obligations arising from the Wwft and the SW, and provide tools for the implementation of these obligations. The Ministry's General Guidance and this DNB Guidance should be read in conjunction with each other.

In this DNB Guidance, reference is made to international (non-binding) guidance documents of the Financial Action Task Force on Money Laundering (FATF), the Basel Committee on Banking Supervision (BCBS) and the International Association of Insurance Supervisors (IAIS). While the guidance documents issued by these organisations are mostly directed at specific sectors, much of the information they contain can also be useful for other sectors. In addition, the documents produced by the Wolfsberg Group can also be useful for some institutions.[3]

1.3 Trust offices and the Regulation on sound operational management under the Wtt 2014

The integrity supervision of trust offices is based on the Supervision of Trust Offices Act (*Wet toezicht trustkantoren* / Wtt). The purpose of the Wtt corresponds to that of the Wwft and the SW. The obligations for trust offices stemming from the Wtt in relation to integrity risks and customer due diligence (CDD) are comparable to the obligations arising from the Wwft and the Wft as regards integrity of business operations.

Trust offices may be affected by the customer due diligence provisions of both the Wwft and the Wtt. When providing services qualifying as trust services under the Wtt, the provisions of the Wwft relating to the customer due diligence do not apply. The Wtt and the underlying Regulation on Integrity of Business Operations under the Wtt (*Regeling integere bedrijfsvoering Wtt 2014* / Rib Wtt 2014) contain a specific framework for trust offices for this purpose, the design and tenor of which correspond with the framework from the Wwft.

It is possible that a trust office with a Wtt permit also performs services that do not qualify as trust services. For example, in practice trust offices sometimes provide domicile for clients. This service does not qualify as a trust service if the activity undertaken by the trust office is limited to providing the address to the client, and the requirements of the Wtt therefore do not apply in this case. The service does however fall within the scope of the Wwft: the trust office qualifies as a provider of domicile under the Wwft, and the regulatory framework of the Wwft applies to the provision of domicile services.

On 1 January 2015 the new Rib Wtt 2014 entered into force. The former supervisory regulation of DNB, known as Rib Wtt, has been elevated to the level of a ministerial regulation. [4]

The Rib Wtt 2014 provides a large number of new regulatory elements compared to its predecessor. In practice, trust offices will fall within the scope of two different laws, the Wwft and Wtt. Within the scope of the Wtt, there is a further distinction depending on whether the trust office provides services to a customer only or to a customer and an object company as well. When applying the present Guidance, it is important for trust offices to keep in mind which specific Act and section apply in which specific situation.

Trust services are defined in Section 1, subparagraph d, of the Wtt. Before providing any such services, a trust office must have obtained authorisation and must have performed a CDD examination in compliance with Section 13 Rib Wtt 2014. If the services involve an object company, an additional examination must be performed pursuant to Section 19 Rib Wtt 2014.

The CDD examination under the Rib Wtt 2014 is in many respects similar to the CDD examination described in the Wwft. The examination of the object company closely resembles the examination that used to be required under the old Rib.

Trust offices carrying out CDD examinations may use this Guidance in the practical set-up and performance of such examinations. The examination of the object company is also discussed, but most of the detail is provided in dedicated boxes.

Where a trust office does not provide trust services, the Wwft continues to have full effect and trust offices may rely on this Guidance in implementing their CDD examinations.

[3] The Wolfsberg Group is an association of eleven global banks, which develops financial services industry standards for 'Know your Customer', anti-money laundering and counter-terrorist financing policies.
[4] Overdrachtsbesluit 2012 integere bedrijfsvoering Wet toezicht trustkantoren.

Chapter 3 of this Guidance is entirely applicable to the implementation of the risk analysis as required under Section 4 of the Rib Wtt 2014.

In addition to this Guidance, DNB has also published several Q&As on its Open Book on Supervision website which trust offices may refer to when implementing the new rules in their operational processes.[5] These Q&As relate to operational policies and set-up (internal operations risk analysis, implementation of the compliance and audit functions) as well as to service provision (service provision risk analysis, performance of CDD and origin of assets examinations, examinations into the purpose of a company's structure, service provision to PEPs).

[5] www.toezicht.dnb.nl/en/4/4/4/51-204404.jsp

2. REGULATORY FRAMEWORK FOR INTEGRITY

2.1 Integrity of business operations

The integrity of financial institutions is one of the pillars of trust and is thus a prerequisite for an institution's proper functioning. It is therefore no surprise that integrity is an explicit norm within financial supervision: Sections 3:10 and 3:17 of the Wft and Section 10 of the Wtt set out the statutory requirements for monitoring integrity of business operations. The key here is that institutions should avoid becoming involved in acts that are against the law and/or are regarded as improper in society, and that they safeguard the integrity of their business operations.[6] Controlling integrity risks is a central tenet of the transposition of this norm into practical rules in the Decree on Prudential Rules under the Financial Supervision Act (*Besluit Prudentiële Regels Wft* / Bpr) and the Regulation on Integrity of Business Operations under the Rib Wtt 2014 . Integrity risks are understood among other things as the risk of money laundering and the risk of terrorist financing. In essence, the Regulations (Wft/Bpr, Wtt/Rib Wtt 2014) prescribe a control framework for this, aimed at controlling integrity risks.

As a minimum, the control framework for integrity risks comprises the following

- Systematic assessment of integrity risks.
- Formulation of a strategy.
- Adoption of an adequate policy aimed at risk control and integrity of action.
- Translation and implementation of the policy principles into procedures and measures.
- Systematic testing and assessment of the adequacy of the control environment, if necessary followed by modifications to that control environment.

Attention for 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. The DNB Suitability Policy Rule 2012 stipulates that the management of institutions must among other things be suitable with regard to the integrity of business operations 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 or strategic reviews. Management must also guard against the institution accepting customers or providing products and services of whom or which the institution has no knowledge or experience, and should ensure that sufficient account is taken of integrity risks in the development and pre-introduction phase of new products and services.

2.2 Ethical business culture

An ethical business culture and ethical conduct are vital to the effectiveness of integrity control measures. Ethical conduct is a professional, individual responsibility in which the individual is aware 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 their decisions and actions. An ethical culture denotes a climate and atmosphere in which a firm behaves or acts, including in a broader sense, in a way that it can explain and account for – not just according to the letter of the law, but also in the spirit of the law.

2.3 Know your customer: customer due diligence (CDD)

In order to guarantee integrity of business operations, it is essential that institutions know who they are doing business with or who they are effecting a business transaction for. The Wft and Wtt therefore impose an obligation on institutions to operate an adequate CDD system in order to know their customers and to avoid engaging in business relationships with persons who could damage trust in the institution. Customer due diligence standards are relevant not only for ensuring the integrity of the business operations of institutions as a whole, but also specifically for combating money laundering and terrorist financing. This is the raison d'être of the Wwft, the law whereby the Netherlands implements the EU directive for the prevention of money laundering and terrorist financing,[7] which in turn is based on the recommendations of the FATF. As the Wft (integrity of business operations), the Wtt and the Wwft are all focused on the same goal, the measures taken

[6] See also Section 2(c) of the Regulation on Integrity of Business Operations under the Wtt (Regeling Integere bedrijfsvoering Wtt), which describes how DNB defines 'integrity of business operations' for trust offices.
[7] Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

under the three Acts can be integrated and the requirements of the three Acts can be met in a uniform manner.[8] The principal goal remains that the institution should know who it is doing business with and for what purpose the business relationship is used.

An institution's CDD policy incorporates procedures, processes and measures in relation to:

- The identification and verification of the identity of customers;
- The acceptance and risk assessment of customers;
- The monitoring of customers, accounts and transactions.

International Guidance

- **BCBS**, Sound Management of Risks Related to Money Laundering and Financing of Terrorism, January 2014, http://www.bis.org/publ/bcbs275.pdf
- **IAIS**, Application Paper on Combating Money Laundering and Terrorist Financing, October 2013, http://iaisweb.org/index.cfm?event=openFile&nodeId=34107
- **IAIS**, Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism, October 2004, http://iaisweb.org/index.cfm?event=openFile&nodeId=34267

2.4 Sanction regulations

The Sanctions Act 1977 (SW) and the regulations derived from it transpose international sanction regimes, especially those of the United Nations and the European Union, into Dutch law. Provisions in these international sanction regimes are transposed into nationally applicable standards via the Sanctions Act 1977. Infringement against these standards is deemed an offence under the Economic Offences Act (*Wet op de Economische Delicten*). The emphasis is on making it a criminal offence to contravene provisions that have been laid down in European Regulations. The Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling Toezicht Sanctiewet 1977*), prepared jointly by the Netherlands Authority for the Financial Market (AFM) and DNB, provides financial institutions with a framework for taking measures. There are two types of financial sanctions: an order to freeze assets and a ban or restrictions on providing financial services. These sanctions are intended to prevent undesirable transactions (embargoes) and to combat terrorism. Institutions take measures to ensure that they can identify relationships who correspond with 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 those relationships and that they are able to freeze their financial assets. Chapter 9 further addresses the sanctions regulation.

2.5 Foreign branches and subsidiaries

Local laws and regulations to promote integrity of business operations or, more specifically, to prevent money laundering and terrorist financing, may differ markedly between jurisdictions. Internationally operating institutions set global minimum standards for the implementation of integrity policy and procedures, which are applicable to the entire group. This means that the integrity control measures will in any event apply to all business operations, all functional activities, and all customers and products worldwide. An institution may operate in jurisdictions (non-Member States) where local laws and regulations set lower integrity standards than the institution's global minimum standards. Institutions will then apply the group's higher standards to the offices and branches in those jurisdictions. If local laws and regulations impose higher standards for integrity control measures than the minimum standards, the institution will reassess its minimum standards and adjust them where necessary.

[8] See the letter from the Minister of Finance to the Dutch Parliament dated 15 October 2008 (Parliamentary Paper 31237, no. 9)

3. PRACTICAL DESIGN OF INTEGRITY POLICY: RISK-BASED APPROACH

The regulatory framework for an adequate integrity policy, and more specifically for controlling the risk of money laundering and terrorist financing, is risk-based. This means that institutions apply all measures prescribed by the law. However, they gear the intensity with which they do so to the risks posed by certain customers, products and services, as well as the combination of certain clients and products, and the delivery channels used (which is the means by which customer contact normally occurs). Within the framework of the Wft (integrity of business operations), Wwft and the Wtt, institutions are expected to classify their customers into risk categories on the basis of the nature and level of the risk they present. This emphasises the responsibility of institutions, which assess the relevant risks themselves and then take adequate mitigating measures. These risk categories vary from low to high-risk, and the classification is based on objective and identifiable indicators. The higher the risks, the more efforts the institution should make to mitigate them.

International Guidance
The **FATF** has published detailed guidance papers for a risk-based approach on a sector-by-sector basis: http://www.fatf-gafi.org/documents/riskbasedapproach/

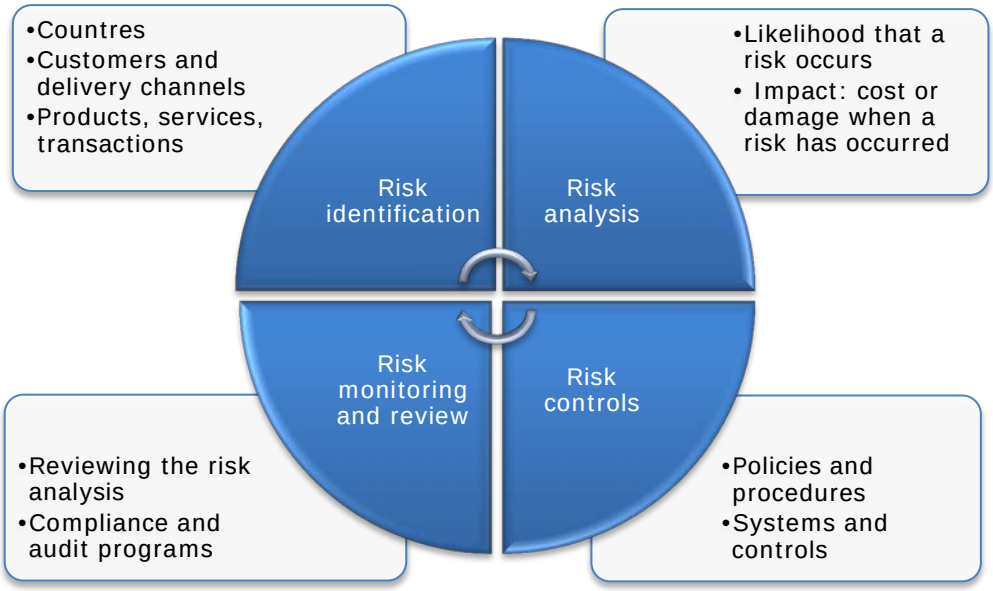
The latest paper in this series is entitled *Risk-Based Approach for the Banking Sector*, October 2014

3.1 Design of systematic integrity risk analysis

Institutions' integrity policy and its implementation begins with a risk-based approach to identifying the risks to which they are exposed. Risks are not static: both internal and external factors can cause the risks for an institution to change. For example, the activities of the institution may be expanded, certain trends may occur within the financial and economic world, or legislation and regulations may be amended. The institution must also determine whether the proposed risk control measures are effective. If they are not, the institution amends them. If an institution cannot control identified risks concerning a certain activity, the institution will adjust that activity or will end the activity. All this means that institutions need to carry out a systematic assessment of the integrity risks; this is an obligation that stems from the Wft and the Rib Wtt 2014. The method used by the institution depends on the specific characteristics of the organisation, such as the size and structure of the institution, the national and international markets in which it operates and the activities it performs. As a minimum, a systematic integrity risk assessment means that the institution performs the assessment periodically in accordance with a predetermined protocol. The institution also records the findings in writing.

The assessment of integrity risks comprises four steps:

1. Identifying the areas of the service provision that are vulnerable to money laundering or terrorist financing;
2. Performing a risk assessment to determine the likelihood and impact of money laundering or terrorist financing;
3. Designing and implementing the risk management process; and
4. Monitoring the risks and reviewing the risk assessment.



3.2 Relevant risks

The institution's customers, services, products and delivery channels are the starting point for the identification of integrity risks. Country and geographical risks are also important. These relate to countries and regions where the institution is active itself or where its customers are established or conduct activities. When preparing an integrity risk assessment, the institution looks at the characteristics of different types of customer, such as sectors or professions, residency or assets and source of income. It also looks at how the contact with customers is generally established and how services are offered (the 'delivery channels', e.g. in person or otherwise, via intermediaries, by telephone or online). The services and products offered by an institution can also be classified according to risk. Generally speaking, products with a long term to maturity from which benefits can be realised carry an inherently lower risk, whereas high-value, complex products can present a higher risk because of their complexity or lack of transparency.[9] For examples for each risk category, see the table in Section 3.3. The institution then looks at the risks that stem from the customer/product or customer/country combinations, and takes the findings into account, first, when setting up the systematic integrity risk assessment and again in defining the customer's risk profile and monitoring the relationship. When defining a customer's risk profile, all specific characteristics of that customer are also taken into account. Ultimately, an institution should have insight into the rationality and reality of the transactions and products of a customer.

The weight assigned to each of these criteria in assessing the overall risk of money laundering and terrorist financing may vary from institution to institution. With regard to the inherent and other risks, the institution should assess both their probability and their potential impact if materialised. It is therefore important that institutions make their own judgments regarding the weighting of the risk criteria, obviously bearing in mind the requirements set by the law or regulations. A number of indicators are listed below (not exhaustive and not applicable in every specific situation), which can help institutions determine the risk.

[9] See also Consideration 9 of the Implementing Directive laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (2006/70/EC).

3.2.1 Country or geographical risk

Possible indicators of country or geographical risk

- Countries or geographic areas subject to sanctions, embargoes or comparable measures, for example imposed by the United Nations, the European Union or the United States.
- Countries or geographic areas identified by credible sources (e.g. the FATF, the IMF or the World Bank) as lacking an appropriate system for preventing money laundering and/or terrorist financing. The ICRG (International Cooperation Review Group) process of the FATF provides a useful tool: after each of its meetings (held in February, June and October) the FATF publishes lists of countries which in its opinion lack an adequate system for combating money laundering and terrorist financing. These lists are published on the FATF's website (http://www.fatf-gafi.org), and DNB refers to each update of these lists on its website (also see the Q&A: http://www.toezicht.dnb.nl/3/50-223306.jsp).
- Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities.
- Countries or geographic areas identified by credible sources (e.g., Transparency International) as having a high level of corruption or other criminal activity.
- Countries or geographic areas characterised by political instability.
- Countries or geographic areas that are known as offshore financial centres.

3.2.2 Product/service risk

Possible indicators of product/service risk

- Services identified by internationally recognised and credible sources as being services that are vulnerable for money laundering, terrorism financing and other integrity risks, such as international correspondent banking services, trade finance and (international) private banking activities.
- Services involving trading in and delivery of banknotes and precious metals.
- Services that inherently foster anonymity or can readily cross international borders, such as online banking and other services, stored value cards, private investment companies and trusts.
- New or innovative products or services that are not provided directly by the institution but via the institution.
- Consultancy companies where it is difficult to verify that the transaction is matched by a specific consideration in the form of a service or product.
- Business or commercial real estate activities.
- Transport or export financing or insurance for goods that can be subject to sanctions.

3.2.3 Customer risk

Possible indicators of customer risk

- Customers who conduct their business relationships or transactions (or have them conducted) under unusual circumstances, such as an unexplained geographic distance between the institution and the location of the customer, frequent and unexplained transfers of accounts to different institutions and frequent and unexplained movements of funds between accounts in various geographic locations.
- Customers where the structure or characteristics of the entity or relationship make it difficult to identify the true owner or controlling interests.
- Cash-intensive businesses, such as bureaux de change, money transfer offices, gambling halls, etc, or customer that use high value notes (100, 200, 500 euro).
- Charities and other not-for-profit organisations (especially those operating on a cross-border basis) which are not subject to any form of monitoring or supervision.
- 'Gatekeepers' such as accountants, lawyers or other professionals holding accounts or acting on behalf of their customers, and where the institution relies on the gatekeeper for the supply of information.
- Use of intermediaries who are not (or not sufficiently) subject to anti-money laundering and counter-terrorist financing measures or who are not supervised.
- Customers who qualify as Politically Exposed Persons (PEPs).
- Customers who are active in sectors associated with increased risk of corruption, such as real estate, construction or oil, gas or other energy-industries.
- Customers who receive news coverage related to financial-economic crime issues, since this negative publicity can have an impact on the institution.
- Foreign feeders: customers who are introduced to trust offices by Foreign Service providers, especially from countries with a (presumed) duty of secrecy.
- Several ultimate beneficial owners (UBO) of target companies between whom there is no economic relationship.
- Provision of services to companies with active branches abroad.
- 'UBO-UBO structures' in combination with advisory services or trading activities, possibly via a conduit company. A UBO-UBO structure is one where the UBO of the company providing the (consultancy) service or product is the same natural person as the UBO of the company that makes the payment (company receiving the service/product).

3.2.4 Delivery channel risk

Potential indicators of delivery channel risk:

- The customer is not present in person when entering into the business relationship.
- The customer is introduced by a third party and the institution is unaware whether that third party is subject to obligations equivalent to those under the Wwft.
- Customer contacts take place mainly through agents or intermediaries, leaving the institution in uncertainty as to whether all relevant information is obtained.

3.3 Division 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 that could influence the integrity risk posed by a business relationship with a customer.

Potential risk indicators of a business relationship with a customer

- 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 degree to which the customer falls under specific supervision (e.g. a financial institution);
- The intensity and duration of the customer relationship;
- Knowledge of the customer's background, such as country of origin; and
- The use of 'corporate vehicles' or other structures that have no demonstrable (commercial) purpose and create complexity or lack of transparency.

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 matches the nature, size and complexity of its customers, products and services.

Example of possible risk classification

Risk category	Examples
Low risk	• Standard services for private customers (savings accounts, salary accounts, credit card payments for small amounts, etc.) • Standard services for small business customers (current account facilities, etc.) • Life insurance products with a low annual premium or low single premium (see also Section 7(1)(a) of the Wwft) • Certain lease products • Pension products (see also Section 7(1)(b) of the Wwft.
Moderate risk	• Accounts and routine international documentary or other payments for medium-sized and large companies • Routine and standard private banking products and services • Correspondent banking accounts for banks subject to legislation equivalent to the Wwft
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, countries which as part of the ICRG process appear on the FATF watch list • Customers with frequent, non-routine, complex treasury and private banking products and services • Non-routine, cross-border payments by non-customers • Correspondent banking accounts with banks from jurisdictions that are weakly regulated in terms of combating money laundering and terrorist financing

3.4 Customers and products with a heightened integrity risk

Certain types of customers or products may inherently carry a heightened integrity risk. These types may emerge from the institution's own risk assessment - for example, operators of coffeeshops or sex clubs: the large amounts of incoming cash, the origins of which are less easy to determine, means that the institution needs to take additional measures for these kinds of customers in order to mitigate the integrity risk. These measures might include setting a limit for

cash transactions and requiring cashless payment in most cases. A heightened risk does not therefore automatically mean that these types of customers have to be rejected.[10]

Based on Section 8 of the Wwft, the legislator may designate certain categories of business relationships and transactions as carrying a heightened integrity risk. DNB may also issue a policy stating the activities where it perceives a heightened risk. Commercial real estate activities are a good example of this, because by their nature they carry a higher risk of fraud and money laundering in view of the relatively high value of real estate, the often non-transparent pricing and the complexity of transactions. In 2011, DNB issued the Policy Rule on Integrity Policy Regarding Commercial Real Estate Activities as a response to real estate fraud. 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 in relation to real estate

- **FATF**, 'Money Laundering and Terrorist Financing through the real estate sector', 2007, http://www.fatf-gafi.org/topics/methodsandtrends/documents/moneylaunderingandterroristfinancingthroughtherealestatesector.html
- **Financial Expertise Centre**, Real estate project report ('Rapportage project vastgoed'), 2008, http://www.fec-partners.nl/media/23/70/811531/18/rapportage_project_vastgoed.pdf
- **Financial Expertise Centre**, 'Red Flags for real estate abuse - update 2010 (´Red flags Misbruik Vastgoed-actualisering 2010´), June 2010, http://www.fec-partners.nl/media/23/70/811531/29/red_flags_misbruik_vastgoed_actualisering_2010.pdf

3.5 Failed customer due diligence and/or unacceptable risk

It can and does occur that an institution concludes on the basis of a risk profile or the application of regulations that an existing or prospective relationship with the customer carries too high a risk. It can also occur that the customer due diligence procedure fails and the institution is thus unable to determine precisely who its customer is and/or what the purpose of the proposed business relationship is. While the failure of a customer due diligence procedure will often (although not always) occur during the acceptance phase, an institution may identify potentially unacceptable risks during a periodic review of the customer's risk profile.

In both cases, the institution does not embark on a business relationship with the customer, or breaks an existing relationship at the earliest opportunity. This obligation stems from Section 5(2) of the Wwft (see also Section 4.2.2 of this Guidance). If the institution suspects money laundering or the financing of terrorism, 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 ended properly, the institution formulates a customer exit policy. Among other things, this policy states the circumstances under which the relationship with the customer will be ended, and the procedure for doing so.

[10] See also the letter from the Minister of Finance to the Dutch Parliament dated 18 January 2010, stating which agreements had been made with the Netherlands Bankers' Association (*Nederlandse Vereniging van Banken* / NVB) with respect to payment facilities for integrity-sensitive sectors (https://zoek.officielebekendmakingen.nl/kst- 27863-35.html).

(Potentially) 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 in a jurisdiction where they have no physical presence);
- Customers whose name corresponds to a name on the EU sanctions list;
- Customers with respect to whom it appears, based on further information, e.g. from EVA, VIS or otherwise, that the combination of customer and products to be used entails unacceptable risks;
- Customers who are not willing to provide information or who provide insufficient information (or submit inadequate documentation for verification purposes) about their nature and background, in particular the source of their assets (or the origin of the funds for the purpose of the Wtt);
- The customer's organisational structure and/or the purpose of the structure of which the object company is a part is (are) found upon examination to be complex or non-transparent, given the nature of the customer's activities, without there being a logical commercial explanation for this;
- Professional counterparties who lack the required authorisation, referred to as ‘illegal financial undertakings’. N.B.: 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.

4. CUSTOMER DUE DILIGENCE

The Wwft makes it mandatory for institutions to carry out customer due diligence in a risk-based manner. This means that the institution carries out customer due diligence in all cases, but that the intensity of the due diligence is determined by the risks associated with certain types of customers, products or transactions. Institutions should take additional measures in cases where there is a higher risk of money laundering or terrorist financing. All this emphasises the responsibility of the institution: the institution is aware of the techniques used in money laundering and the financing of terrorism, of current developments and of risk indicators, and has incorporated these in policy and in risk-based procedures and measures.

Customer due diligence enables the institution to identify the customer, verify their identity, identify the ultimate beneficial owner of the customer and verify the ownership and control structure of the group to which a customer belongs, determine the purpose and envisaged nature of the business relationship and investigate the source of the assets used in the business relationship or transaction. The institution also looks at whether the customer is acting for itself or on another party's behalf, and whether the person concerned is the authorised representative. The institution should also monitor the customer's activities during the relationship and check periodically whether the customer still meets the risk profile that was established at the commencement of services. At the inception of a customer relationship, the institution should have gathered sufficient information to be able to accept the customer on the right grounds. The various aspects of customer due diligence are discussed below.

4.1 Identification and verification

4.1.1 General

The Wwft uses a broad definition for the term 'customer': the customer is the natural or legal person with whom a business relationship is entered into or who has a transaction effected. A customer is any party with whom an institution enters into a business, professional or commercial relationship that is connected to the professional activities of the institution. The professional activities include the institution's primary activities for which a licence was granted. However, if the institution offers certain activities that have a financial aspect with a risk of money laundering or terrorism financing, the institution will apply the Wwft to these activities. An example is transactions for telecom-companies (related tot text or '0900'-services) that are provided by payment service providers.

This means that relationships with professional counterparties in the context of the core activities of the institution, such as relationships with financial institutions and financial service providers, also fall under the Wwft definition.

Identification and verification of the customer
Customer acceptance, identification and verification are generally defined as follows:

***Customer identification*:** the process whereby the customer's data and information are collected with the objective to 'know your customer'. The data allow an adequate and robust risk assessment to be made of the customer.

***Verification*:** the process whereby the accuracy of customer-submitted and other data is checked using a reliable and independent source, e.g. in the form of original and valid identity documents and possibly supported by further investigation.

***Customer acceptance*:** the process whereby, based on the identification, verification of identity and knowledge of the nature and background of a customer, a decision is taken about whether or not to enter into a relationship with the customer.

For identification purposes, the customer should submit proof of his/her identity. The verification process is intended to determine whether the proof of identity submitted matches the customer's real identity. On the basis of documents, data or information from credible and independent sources, the institution checks the accuracy of the proof of identity submitted by the customer. Section 4 of the Regulation implementing the Wwft (*Uitvoeringsregeling Wwft*) mentions a number of documents that can be used for this purpose.

Other documents, information or data can also be accepted for the purpose of verifying the identity of a natural person, provided they originate from a credible and independent source. An example is the verification of identity of a natural person from a non-Member State who is not in possession of a passport. Accounts in the name of the person in question, possibly in combination with other data on that person, may in some cases be accepted. This is a matter for the risk assessment of the institution wishing to accept the relevant person as a customer. Institutions are quite capable of making such evaluations as, within the scope of covering their business operations risk, they will also want to know who the customer is.

The identity of foreign legal persons is also verified on the basis of documents, data or information from a credible and independent source which is usual in international dealings. Comparable documents may also be requested for this purpose to those used for the verification of Dutch legal persons as described in Section 4(3) of the Regulation implementing the Wwft (*Uitvoeringsregeling Wwft*), provided these are recognised as means of identification in the customer's country of origin.

If documents do not originate from public authorities or the courts, the institution will question whether the documents are sufficiently reliable. Normally, such documents will in themselves be insufficient to verify identity adequately. Documents in respect of which it is not certain that they are based on adequate identification and verification, such as student and staff passes, generally do not suffice to verify identity.

4.1.2 Front men

In the process of customer due diligence, the institution also looks at whether the customer is acting for himself or for someone else. The aim is to assess whether someone is acting as a front man in their own name but on behalf of (criminal) third parties. If it is clear that the customer is acting for someone else, such third party qualifies as “client” (“the natural or legal person [...] who has a transaction effected”) so that the CDD obligations of Section 3 of the Wwft apply with regard to that person.

Otherwise, a risk-based approach can be used: the institution draws up a set of indicators that make it possible to determine whether someone is acting for themselves or for someone else. These indicators may include instances where the person is unable to answer certain questions, for example about the origin of the funds, or where unclear, vague reasons are given for the transaction. In case of suspicion that the customer is a front man, the institution automatically also examines whether there is a heightened or acceptable risk, taking into account the characteristics and where possible the identity of the person(s) on whose behalf the customer appears to act.

4.1.3 Representatives

Where a natural person purports to act as a representative of a customer, the institution also checks whether this person is authorised to represent the customer, for example where a natural person purports to act as the director of a legal person. Where a natural person claims to indirectly represent a legal person (which legal person would be the customer), the chain of representative authority is established. If such authority is established, the customer will be the subject of the customer due diligence measures of Section 3 of the Wwft, while the natural person acting as representative will be identified and his identity verified (Section 3(2)(g) of the Wwft). If the representative is not seen in person, the institution can develop a procedure to establish with certainty who acts for the customer and to verify that the person concerned is duly authorised. The institution will then in any event require a declaration of identity from the officers of the customer with whom it has direct contact, including those with whom it develops the procedure referred to, and will verify that declaration.

4.1.4 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 has a transaction 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. The 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. When establishing the control structure, persons who are authorised to manage the partnership also fall under the customer due diligence, and the institution identifies them. The institution takes risk-based and adequate measures to verify the capacity of these persons as partners. The identity of the natural persons who qualify as equivalent to ultimate beneficial owners is verified using a risk-based approach. Verifying the identity of all partners will in some cases be impossible in practice, for example in the case of an 'open limited partnership'.

4.1.5 Trusts

A trust is a foreign legal form that cannot be incorporated under Dutch law, but which is recognised in the Netherlands. A trust does not possess legal personality and is therefore not the party with which a business relationship is entered into or that has a transaction effected. Consequently, a trust does not qualify as a customer. The trustee is regarded as the customer. The obligations pursuant to the Wwft therefore relate to services carried out for a trust. In the case of a trust, the usual steps must be taken in respect of customer due diligence, but the founders of the trust, the trustees, the protector and the beneficiaries must also be known to the institution. The customer must submit a statement of their identity and the institution must verify these stated identities.

4.1.6 When identification and verification must be carried out

Section 3 of the Wwft stipulates the occasions on which customer due diligence must be performed. These include cases where an institution enters into a business relationship or carries out a (set of) transactions above a specific limit.

Identification and verification by trust offices

Pursuant to Section 3(13) of the Wwft, paragraphs 2-6 and 8 of Section 3 do not apply to trust offices in so far as they perform certain trust services. The simplified customer due diligence referred to in Section 6 of the Wwft and the enhanced customer due diligence referred to in Section 8 of the Wwft therefore also do not apply for trust offices. The Wtt and the Rib Wtt 2014 set the customer due diligence requirements for trust offices.

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 EUR 15,000. This will be assessed by the institution on the basis of the type of transaction and the amounts involved. To begin with, they should be one-off transactions, which means that no business relationship exists. It is also logical that the transactions should be similar in nature: for instance, someone who, through several transactions conducted in a single day or within a few days, makes cash payments into an account without being its account-holder (or acting on behalf of the account-holder), the overall amount of which exceeds EUR 15,000. By contrast, this provision is not applicable to a company that pays the cash proceeds from its regular business operations into its own account daily, as such payments are made as part of the business relationship.

An institution which carries out money transfers will not always enter into a business relationship with a customer as defined in the Wwft. Legislative history, however, shows that a business relationship may be assumed to exist in the case of money transfers.

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;
- the institution doubts the reliability of information obtained previously 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 country where the customer lives;
- a one-off electronic money transfer is effected.

Given the undiminished vulnerability, institutions that transact money transfers also perform the customer due diligence.

In principle, identification and verification are completed before the business relationship is established and the service provision commences. However, there are exceptions in cases where the provision of services, e.g. advisory services to customers, should not be interrupted.[11] In these exceptional cases, the purpose of the law should still be kept in mind, viz. to prevent the institution's services from being used for money laundering or terrorist financing. This is subject to the condition that the risk of money laundering or terrorist financing is low and that the institution will verify identity as soon as possible after the first contact with the customer.

One may think of situations where the nature of the institution or of the services offered creates technical or organisational reasons why preliminary and limited services may be provided. An example is a payment service provider facilitating online transactions for retail merchants. Owing to the design of the service provision, some limited form of service provision may be commenced before the verification process has been completed. However, such necessary initial service provision may take place only in low-risk situations. This implies that the institution must perform a preliminary risk estimation to assess whether the risk of money laundering or terrorist financing is sufficiently low. Examples of indicators to be used in such an estimation exercise are the customer's country of origin, the customer's line of business or the product the customer intends to purchase. The institution remains obliged, of course, to complete the identification and verification process as soon as possible after the initial contact.

Banks 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.[12] This also applies to credit cards issued by banks. As long as the credit card is blocked (comparable to an account that cannot yet be used), the bank 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 should have been completed.

Similarly, on taking out a life insurance policy, it is permitted to identify the policy's beneficiary and verify his/her identity after the business relationship has been entered into. In that case, identification and verification of identity should take place on or before the time of payout, or on or before the time that the beneficiary wishes to exercise his/her claims under the policy. The payout to a beneficiary of a life insurance policy is not an occasional transaction, but is the result of the business relationship into which the institution has entered the policyholder. If the beneficiary is a legal entity, the ultimate beneficial owner will also be identified and his/her identity verified, using risk-based and adequate measures.

For customers who have already been identified pursuant to the Identification Services Act (*Wet Identificatie Dienstverlening, WID*) or for whom that law did not require identification, Section 38 of the Wwft and the royal decree based thereon stipulate time limits within which customer due diligence must in any case be applied[13] These time limits are set for customers who live in certain designated countries; customers presenting a higher risk or politically exposed persons to whom the enhanced customer due diligence applies; or to foreign legal persons or

[11] Section 4(2) of the Wwft.
[12] Section 4(4) of the Wwft.
[13] Section 38 and the Royal decree: "Besluit van 9 december 2013 tot vaststelling van het tijdstip bedoeld in artikel 38, eerste lid van de Wwft", Staatsblad 2013, no. 544.

persons acting for a trust. For other customers, to whom these three situations do not apply, the institution carries out the customer due diligence procedure at the first opportunity.

Examples of triggers for a customer due diligence procedure carried out for customers, who have already been identified in pursuant to the WID:

- a customer is considered as higher risk.
- a customer is due for a review according to the review process established within the institution;
- the institution becomes aware that it lacks sufficient information about the customer;
- there is a material change in the way that the customer's account is operated;
- the customer documentation standards change substantially;
- the customer purchases a new product or service;
- a transaction of significance takes place;
- in the event of contact with the customer which presents an opportunity to carry out the customer due diligence.

In the case of life insurance contracts, the customer due diligence for a customer who has already been identified pursuant to the Identification (Financial Services) Act will be performed in all cases where a financial payment is made to the customer.[14]

4.2 Entering into a business relationship

With due observance of the exception described above, an institution may only enter into a business relationship if it has conducted the full customer due diligence procedure, the due diligence has led to the envisaged result and the institution is in possession of all identification and verification details and other information. An institution need not carry out the customer due diligence itself, but can arrange for this to be carried out by another institution.
An institution may rely on these data because these designated persons and the institutions themselves are institutions in the sense of the Wwft.

The Explanatory Memorandum to the Act recommends that the introducing institution should keep (copies of) the relevant documents available to show to the recipient institution at its first request. It is however more practical to make the information available to the recipient institution immediately on introduction, because the institution must itself possess the data and is also itself responsible for compiling the risk profile, for which it requires the correct information. If the introducing institution cannot provide the information, the other institution will conduct the customer due diligence if this is necessary pursuant to the Wwft or the internal rules.

If the other institution has carried out the simplified customer due diligence for a customer because that customer purchased a low-risk product, the institution relying on the other institution can still ask the introducing institution for further identification and verification details. An institution may always do more on the grounds of its internal procedures than the Wwft requires, and may therefore also decide to perform a customer due diligence. The simplified customer due diligence is not possible where there is a suspicion of money laundering and terrorist financing. If the institution to which a customer has been introduced harbours such suspicions, the institution has an extra reason for requesting the data.

An institution relying on the identification and verification of identity by another institution governed by the Wwft will proceed carefully. As responsibility for maintaining an accurate customer file lies with the institution itself, it is important that the institution assures itself that the relevant elements of the customer due diligence procedure have been carried out in accordance with the Wwft (or comparable legislation in international situations), and that the other institution has in place adequate procedures and measures in relation to the Wwft. This means that the procedures of the introducing party should be adequate in terms of their design and operation. If an institution repeatedly accepts customers from the same other institution, it is logical that it requests and assesses the Wwft procedures of that institution in a risk-based way. In the case of new business alliances, the Wwft procedures should always be requested for assessment.

This is relevant in particular for life insurers who rely on customer due diligence performed by financial service providers acting as life insurance brokers. The insurer is responsible for adequate implementation of the Wwft policy. Specifically, this means that the insurer formulates a customer

[14] Section 38(2) of the Wwft.

identification and verification policy, setting out the procedure in relation to reliance on customer identification and verification as carried out by the relevant financial service providers. In addition, policy is formulated whereby the relevant financial services providers make customer identification data immediately available on request. Financial services 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, the insurer still carries its own responsibility in this respect. It may for instance only sign an insurance contract after making sure that the insurance broker has determined and verified the customer's identity. Insurers should carry out periodic risk-based checks to ascertain whether the relevant financial services providers have measures in place to enable adequate 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 services 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.

4.2.1 Periodic update and review

The institution compiles a risk profile of the customer based on the customer due diligence. This risk profile is dynamic, and can therefore change over time. A review serves to determine whether the customer still meets the defined risk profile. To that end, the institution should periodically update all customer data, including the customer's risk profile, contact information and ultimate beneficial owner(s). The basic principle is that the frequency and depth of the review depend on the risks presented by the customer.

When is the customer due diligence reviewed?

For **low-risk customers**, a review may take place when:

- the customer requests a new service or product, or in the case of customer contact which presents an opportunity to carry out the customer due diligence procedure;
- 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 of the specific risks will in practice be carried out (once or several times per year) and, for example, in the case of:

- possible signs suggesting a higher risk. Examples are the manner in which accounts are used or specific transactions are effected, as viewed from the consolidated position of the customer in question.

In all cases, the employees involved are aware of the possible risks surrounding this type of high-risk customers.

In their policies and procedures, institutions set out the frequency with which and way in which the customer data are updated and how the periodic reviews of the customer's risk profile are conducted and data kept up to date.

4.2.2 Prohibition on entering into a business relationship

Pursuant to Section 5 of the Wwft it is prohibited to enter into a business relationship or carry out a transaction if no customer due diligence has been performed or if the customer due diligence, including the review of the ultimate beneficial owner, has not produced the intended result. There is a statutory obligation to terminate the business relationship if it is not possible to comply with statutory obligations. An institution reports these instances to FIU-NL if there are also indications that the customer is involved in money laundering or terrorist financing.

If unable to terminate the business relationship, the institution should take further adequate measures to perform customer due diligence.

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

The Wwft also includes a ban on entering into a correspondent banking relationship with a shell bank.[15] It is also not permitted to enter into or continue a correspondent banking relationship with

[15] Shell banks are defined in Section 1(1)(j) of the Wwft.

a bank which is known to allow a shell bank to use its accounts. Shell banks entail risks because of the nature of their organisations. They offer services in a country without having a physical presence in that country, i.e. there is no presence of governance or management in that country. The conduct of such institutions is difficult for supervisory authorities to monitor.

4.2.3 Protected accounts

According to international standards on customer due diligence and on combating money laundering and terrorist financing, institutions are not permitted to maintain relationships with persons who remain anonymous or persons who provide fictitious identity details. As in a limited number of cases it may be useful to protect a customer's identity internally – 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 (*Regeling afgeschermde rekeningen Wft*)[16] provides for a procedure in which the customer's identity is not visible or is otherwise protected during transaction processing. While the customer is known to the institution, not all staff members are aware of his/her identity.

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 keep 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 transaction processing. The requirements under the Wwft regarding customer due diligence remain fully applicable, as does Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds.

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 ought to be particularly alert if a customer requests a 'in name of' account with an account name that cannot be explained. During the periodic review, it is possible that such an account goes 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.

4.3 Ultimate beneficial owner

The institution should for every customer identify the ultimate beneficial owner (UBO). The ultimate beneficial owner is always a natural person. This requirement is not only relevant when the customer is a legal entity, such as a legal person, foundation or trust: if the customer is a natural person over which another natural person can exercise actual control, then that other person qualifies as UBO. [17] Performing a customer due diligence for the ultimate beneficial owner is a statutory requirement since criminals often use schemes involving (foreign) legal persons as a means of concealing the criminal source of funds. This requirement can be met by having the customer state who the ultimate beneficial owner is. The institution also takes adequate risk-based measures to verify the identity of the customer based on independent and reliable documents. This does not mean that the institution has a choice as to whether or not to verify the identity of the ultimate beneficial owner depending on the risk involved: his/her identity must always be verified, but the way in which the verification is carried out will be risk-based. This means that more measures are taken with respect to high-risk customers than to low-risk customers.

The verification measures should enable the institution to obtain sufficient information to convince itself of the identity of the ultimate beneficial owner. The institution also checks whether the UBO is a PEP (Politically Exposed Person).

[16] See http://www.toezicht.dnb.nl/en/4/4/2/51-204124.jsp
[17] See the definition of UBO in Section 1(1)(f)(3) of the Wwft.

Which independent and reliable documents can be used to verify the identity of the ultimate beneficial owner (UBO)?

- Public registers and other sources (see the 'General Guidance on the Anti-Money Laundering and Counter-Terrorist Financing Act (Wwft) and the Sanctions Act (SW)' by the Ministry of Finance for further information and examples);
- Relevant details or documents from the customer.

The following verification measures can be taken for low-risk customers:

- Asking about the identity of the UBO, and having the UBO and/or the customer's representative sign a declaration.
- For a majority shareholder-director, an extract from the Trade Register can be used showing the name of the 100% shareholder.

Institutions should also have adequate risk-based measures in place to provide an insight into the customer's ownership and control structure in the case of legal persons, foundations, trusts and other legal arrangements. This includes measures to verify the legal status of customers other than natural persons, if possible by obtaining proof of incorporation.[18] 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 should devote more efforts to understand the domestic and/or (international) shareholder 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. This can be achieved by inquiring with the customer, but also by requiring a legal or tax opinion or advice.

The concept of 'ultimate beneficial owner' as defined in the Wwft is not suitable for use in the context of unincorporated partnerships. For example, an unincorporated partnership has no shares or general meeting. The Wwft adheres as closely as possible to the elements forming part of the concept 'ultimate beneficial owner'. Among other things, this means that instead of voting rights in a general meeting, the Wwft takes as a basis voting rights in decisions on amending the agreement that underlies the partnership or the performance of that agreement other than through management acts. This aspect of the customer due diligence focuses on the influence on more radical decisions by the unincorporated partnership in respect of special transactions (falling outside the scope of the normal business operations) or amending the agreement that underlies the partnership (e.g. as regards the distribution of profit). The natural person who is able - directly or indirectly – to exercise effective control over the partnership is regarded as the equivalent of the ultimate beneficial owner.

UBO-related requirements for trust offices

The obligation for trust offices to identify the ultimate beneficial owner is enshrined in Section 10 of the Wtt in conjunction with Sections 13 (customer) and 19 (object company) of the Rib Wtt 2014 if the trust office provides 'Wtt services'.

4.4 Purpose and nature of business relationship

By gathering information about the purpose and envisaged nature of the business relationship, an institution will be able to estimate any risks that may arise from the provision of services to the customer. Usually, part of the required information will already have been obtained during contact with the customer prior to the establishment of a business relationship. Also, the purpose of the relationship will be apparent from the services or products used by the customer. Additional queries from the institution can be aimed at obtaining clarification on the product user or service recipient. For customers not located or residing in the Netherlands, an institution should be clear as to why the customer intends to use its services or products. If that is for tax purposes, the institution assesses the acceptability of that purpose. Or in the case of cross-border money transfers, such as remittances, the purpose of the transaction is evident. In increased-risk situations, purpose and nature inquiries should also establish what type of transactions (including number, frequency and size) the customer intends to perform.

[18] Such verification may take place according to the General Guide to Account Opening and Customer Identification issued by the Basel Committee's Working Group on Cross Border Banking, February 2003 (http://www.bis.org/publ/bcbs85annex.htm).

4.5 Source of funds

The principle when entering into a relationship with a customer is that, if necessary, the institution knows the source of the funds that will be used in the business relationship or transaction. The institution should record statements and documentary evidence in customer files and ask further questions where necessary. The fact that the funds originate from a regulated institution does not imply that the institution itself need not carry out a due diligence review. To determine the plausibility that the funds originate from a legal source, the institution should identify specific indicators which determine the depth of the review. The institution can consider combinations of indicators, such as the amount involved, the reason given for the source of the funds, age and profession or business activities of the customer, country of origin or destination of the funds, and the provided product or service. In the case of life insurance, this could for example mean a very high initial premium or top-up payments. In high-risk situations, especially, it is appropriate that the plausibility of the source of funds be determined and recorded using independent and credible sources.

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 be able to define a correct risk profile. The institution should document its review of the source of funds.

Requirements for trust offices

The obligation for trust offices to identify and record the source of funds is laid down in Section 10 of the Wtt in conjunction with Section 13(2) and 19(2) of the Rib Wtt 2014. A trust office providing services to an object company is thus required, first, to verify the origin of the object company's and UBO's assets and, secondly, to verify the origin and destination of the object company's financial means.

4.6 Simplified customer due diligence

For specific customers, a simplified customer due diligence review may suffice. Section 6(1) of the Wwft describes types of customers that constitute a lower risk of money laundering and terrorist financing and for which a simplified customer due diligence regime applies. They consist primarily of institutions governed by the Wwft or equivalent legislation and customers with a specific legal personality. In addition, Section 7(1) of the Wwft lists a number of products, such as life insurances with low premium amounts, for which a less stringent regime applies.

Institutions should however gather sufficient data to assess whether a customer meets the requirements for the simplified customer due diligence . For instance, the institution may ask for an extract from the Trade Register, entries in public registers or other public listings. Such appraisal is subject to review: Even in these circumstances, the institution is required under Section 3(8) of the Wwft to keep the information on which its conclusion is based up-to-date

Simplified customer due diligence is permitted for specific customers resident in a Member State or for specific customers resident in non-EU Member States as designated in Section 3 of the Regulation implementing the Wwft (*Uitvoeringsregeling Wwft*). However, Section 6 of the Wwft does not render Sections 8 and 9 of the Wwft inoperative. Thus, if there are facts or circumstances which lead to an enhanced risk of money laundering or terrorist financing, the institution will perform an enhanced customer due diligence irrespective of where the customer's registered office is located. This also means that some type of monitoring of these business relationships is always necessary to assess whether the account is actually being used for the reasons given. The Explanatory Memorandum to the Regulation implementing the Wwft (*Uitvoeringsregeling Wwft*) states that an institution is free – based on its own risk assessment – not to perform simplified customer due diligence in respect of an institution resident in one of the equivalent states.

The institution should also assess whether the account is held and used 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 are from the bank's customer or customers and the transactions on the account are carried out for the account and risk of that customer or those customers. In these cases, the institution should 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 the institution 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 a higher risk (pursuant to Section 8 of the Wwft).
As regards third-party accounts held by professionals with institutions, these institutions need not perform customer due diligence on the professional's customers. The institution has already carried out the customer due diligence of the professional (the account-holder) itself. As this professional also falls within the scope of the Wwft, it must in turn meet the obligations set out in Section 3 of the Wwft in relation to the customer due diligence for its customer. It is therefore not necessary for the institution to perform customer due diligence on the 'customer's customer' where professionals are concerned.

Pension funds and non-life insurers are not governed by the Wwft. Institutions having such entities as customers cannot make use of the simplified customer due diligence provision of Section 6(1) (a) or (b) of the Wwft. In cases where such an entity has issued securities that have been admitted for trading on a regulated market in a Member State (Sections 6(1) (c) and 6(1)(d) of the Wwft), however, a simplified customer due diligence will suffice.

Additionally, pursuant to Section 3(6) of the Wwft, institutions may, for this type of supervised institutions, gear the customer due diligence to the sensitivity of the institution to the risk of money laundering and terrorist financing; such institutions will generally entail lower risks. Pursuant to Section7(1) (b) of the Wwft, however, institutions selling pension products to their customers may employ a simplified customer due diligence, unless there are suspicions of money laundering or terrorist financing.

In addition to the products listed in Section 7(1) of the Wwft, reference is made in Section 3 of the Decree containing provisions on the scope of the Wwft (*Uitvoeringsbesluit Wwft*) to products that meet all conditions set out in Section 3(3) of Directive 2006/70/EC. These conditions are highly technical and detailed. It would therefore be unwarranted to provide an exhaustive list of the types of products here. Institutions need to assess this on a case-by-case basis. Naturally, these are products with a low risk of money laundering, such as the examples cited in consideration 9 of the Directive: products for which the benefits cannot be realised on behalf of third parties and can only be realised in the long term. Examples include certain unit-linked insurance or savings products, or cases where the financial product is used to finance tangible assets in the form of a lease agreement in which the legal and economic ownership of the underlying asset remains with the lease company, or in the form of a low-value consumer credit, provided the transactions are effected through a bank account and remain below an appropriate threshold.

4.7 High-risk situations

In cases where there is a higher risk of money laundering or terrorist financing, the institution takes supplementary measures (i.e. in addition to measures taken pursuant to Sections 3 and 6 Wwft). These measures vary according to risk. When accepting customers purchasing a product with an enhanced risk, for example products or combinations of products which deviate from standard products, standard procedures are not sufficient. The institution must therefore do more than simply check whether the customer or other stakeholders appear(s) on the sanction lists, whether they are creditworthy or whether their identity documents are genuine, and whether the customer appears in institutions' internal or external warning systems. Such supplementary 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 about business activities as well as (negative) background information on the client. Also, in the context of enhanced CDD, the institution's examinations of the customer's source of funds should be more profound.

In the case of customer-product combinations with a higher risk, the institution will not simply accept the information submitted by the customer at face value, but will where possible check the information by relying on independent and credible sources, and will in any event carry out a credibility check.

In which situations must the institution always carry out an enhanced customer due diligence?

- The customer is not physically present.
- The customer is a PEP.
- There is a correspondent banking relationship.
- If facts or circumstances, including the country where the customer lives or is established, suggest a higher risk of money laundering or terrorist financing.

Section 8 of the Wwft states which activities an institution can (subsection 2) or must (subsections 3 and 4) undertake to mitigate the higher risk.

The supplementary measures to be taken depend on the institution's risk assessment with respect to the customer, transaction, product or country concerned. Where jurisdictions have been identified by the FATF as jurisdictions that have not set up adequate systems to prevent money laundering and terrorist financing, this must be seen as one of the factors increasing the risk of money laundering and terrorist financing in a business relationship or transaction.[19] In that case, institutions must take additional measures to mitigate the heightened risk. In case the customer is not a natural person, it is up to the institution to take enhanced measures to verify the legal status of that customer. The measures to be taken depend on the risk of the jurisdiction concerned.

Additional information

- **FATF typology reports,** http://www.fatf-gafi.org/topics/methodsandtrends/
- **Egmont Group case descriptions,** http://www.egmontgroup.org/library/cases

NB: The European Banking Authority (EBA) is currently engaged in drafting new guidance on risk factors, which it is expected to release in the course of 2015.

Pursuant to Section 9 Wwft, the Minister of Finance can designate institutions to take additional measures for certain customers and transactions that carry such a great risk that special measures are necessary. These are customers in and transactions relating to states which persistently refuse to implement the internationally adopted FATF recommendations. At present, the FATF has designated two states in this regard: Iran and North Korea.

The law makes explicit which special measures should be taken for customers and their ultimate beneficial owners who live or are established in such countries. For example, additional information is gathered about the purpose and nature of the business transaction, the origin of the funds used in the business relationship or transaction and the source of the assets of those customers and those ultimate beneficial owners. The details of these customers are also regularly updated and the business relationship and associated transactions are subjected to additional checks. Additional information is also gathered about the background to and reasons for the transactions.

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

4.7.1 Customer not physically present

There is a higher risk in cases where the customer is not physically present for the identification and verification of identity. Section 8(2) of the Wwft lists a number of options to offset the higher risk in cases where the customer is not physically present and the institution is unable to verify the customer's identity using the identity documents set out in Section 4 of the Regulation implementing the Wwft (*Uitvoeringsregeling Wwft*).

An institution can also take other measures as long as the higher risk of the customer's not being physically present is mitigated. To that end, the institution can request supplementary documents, data or information. This is supplementary documentation which must be provided in addition to items such as a copy of proof of identity, or a combination of several documents. Examples include bank statements, gas and electricity bills, pay slips and/or employment contracts. It is important

[19] See DNB Q&A on FATF warning lists, http://www.toezicht.dnb.nl/en/3/51-223306.jsp

that these documents are issued by independent third parties (cf. 4(3) of the Regulation implementing the Wwft (*Uitvoeringsregeling Wwft*)).

The institution will assess the documents submitted for authenticity. The institution may for example ask the customer to have copies of the documents authenticated or, for some documents, have them submit the originals (and return these after checking).

The 'name-number check' as described in Section 8(2)(c) of the Wwft is a widely used method to verify identity. However, since pursuant to Section 4(4) of the Wwft the customer's identity must be verified before entering into the business relationship, the institution should ensure that the first payment precedes or coincides with the commencement of the business relationship with and the provision of professional services to the customer. The customer may make deposits into the savings or other account concerned, but the institution will keep the account blocked and will not allow the customer to withdraw or transfer funds before the entire verification process has been completed. To verify the name-number combination, institutions can also perform a direct debit transaction for a small amount. It should be noted that in the context of SEPA-payments, some banks no longer regularly transmit the account name.

In the case of joint accounts, the second account-holder's name is not always stated on the transfer of funds. A (printout or copy of a) bank statement or a copy of the bank card may then be requested in order to verify the full title to the account. In this type of identification it is important that there is sufficient certainty that the customer has provided proof of his/her identity elsewhere and can thus be traced by a paper trail.

4.7.2 Politically Exposed Persons (PEPs)

Business relationships with and providing services to PEPs require additional measures as they entail a higher risk of reputational damage and other risks for institutions. In addition, the provision of services to PEPs demands special attention within the framework of international policy to combat corruption. According to Consideration 25 of Directive 2005/60/EC, business relationships with PEPs, particularly those from countries where corruption is widespread, may expose the financial sector, in particular, to significant reputational and/or legal risks. Examples are passive corruption (taking bribes) or misappropriation of public funds. An institution therefore needs to take risk-based procedures and measures in order to be able to identify PEPs, and consequently determine the source of wealth and of funds that are used with the business relationship or transaction, and keep the business relationship under constant supervision.

PEPs are understood as individuals who are or have been entrusted with prominent public functions, as well as the immediate family members or close associates of these individuals. For the definition of this term, the Wwft refers to Section 2 of Implementing Directive 2006/70/EC, where the term 'politically exposed person' is specified in detail. An individual will remain a PEP until one year after he/she has ceased to hold the prominent public function, position or capacity which caused them to be considered a PEP. The Implementing Directive[20] considers that public functions exercised at levels lower than national need normally not be considered prominent. However, where their political exposure is comparable to that of equivalent positions at a national level, institutions should consider, on a risk-sensitive basis, whether persons exercising those public functions should be regarded as PEPs or as customers with a high integrity risk.

A review is carried out both on acceptance and periodically to determine whether the customer and the ultimate beneficial owner of the customer qualify as PEPs. This applies equally to natural persons who may exert considerable influence on, hold considerable interests in and/or may strongly influence further reaching decisions of the unincorporated partnership, or who are able to control the partnership's policy to an essential degree. The Wwft requires that institutions have in place risk-based procedures and measures for this purpose. The depth of the customer due diligence varies depending on the risk profile of the customer or ultimate beneficial owner. The Explanatory Memorandum to the Act provides a great deal of information on this.

To determine whether a particular customer or ultimate beneficial owner is a PEP, an institution may in low-risk situations consult public sources (such as the Internet) or obtain information from its own branch in the country of residence of the relevant customer. For institutions with a sizeable

[20] Consideration 3 of Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of "politically exposed person" and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

international customer base, it may be efficient to use lists provided by recognised commercial organisations.

Institutions take enhanced customer due diligence measures in the case of transactions or business relationships with politically exposed persons

- who live in a different country or Member State (regardless of their nationality);
- who live in the Netherlands with a non-Dutch nationality.

NB: Life insurers do not need to take enhanced measures for the latter category of PEPs. These institutions do need to carry out a PEP check if the customer or ultimate beneficial owner does not live in the Netherlands or moves abroad.

The additional measures to be taken depend on the institution's risk assessment with respect to the customer, transaction or product concerned. Therefore, when it is known that a customer with Dutch nationality is a PEP residing in the Netherlands, an institution should also carry out a risk assessment regarding the extent to which additional measures may be necessary for this customer.

The decision to enter into a business relationship with a PEP or to conduct a transaction for a PEP should be taken or approved by persons authorised by the institution to do so. This also applies to a decision to continue a relationship with a customer who becomes a PEP. Such approval is granted by senior management.

How should institutions deal with PEPs?

- During the acceptance process, institutions 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 seen as 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 instance, the parents of a member of the board of management of a foreign central bank with an ordinary current account in the Netherlands will be less risk-sensitive than the wife of a head of state of a country with an increased risk of corruption, who opens a private banking account and deposits large sums of money. In the case of PEPs, the institution will not simply accept the information submitted by the customer at face value, but will where possible check the information 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 individual's country of origin, for example by referring to the Corruption Perception Index from Transparency International.

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

Additional information

- **FATF,** Guidance: Politically Exposed Persons (Recommendations 12 and 22), http://www.fatf-gafi.org/documents/documents/peps-r12-r22.html
- **The Wolfsberg Group,** FAQ over PEP's, 2008, http://www.wolfsberg-principles.com/pdf/faq/Wolfsberg_PEP_FAQs_(2008).pdf
- **Transparency International,** http://www.transparency.org

4.7.3 Correspondent banking relationships

Institutions should exercise due care when entering into correspondent banking relationships. Section 8(3) of the Wwft stipulates that banks should obtain a good picture of institutions from non-Member States with which they enter into correspondent banking relationships. In a correspondent banking relationship a bank in reality acts as an agent for another bank by effecting payments or performing other services for a customer of the correspondent bank. To avoid the bank being misused by means of these transactions for money laundering or terrorist financing purposes, it is important that a number of conditions be observed.

Under the law, an institution must perform enhanced customer due diligence if it enters into a correspondent banking relationship with a bank established outside the EU. This does not however mean that enhanced due diligence is never performed when entering into a correspondent banking relationship if the correspondent bank is established in a Member State. If a higher risk of money laundering or terrorist financing could arise in the light of facts and circumstances in a specific case or based on the institution's internal risk classification of countries and jurisdictions, the institution may take additional measures to mitigate this higher risk.

It is particularly important to be alert to the potential use of a correspondent bank account by (unidentified) third parties (transit account or payable-through account), in other words when a customer of the foreign bank has direct access to the account held by that bank at a Dutch bank. The reason why close attention needs to be paid to this category of accounts is that in reality it entails the provision of services at a distance. The correspondent bank itself usually has no relationship with the parties involved in the transaction and thus has less opportunity – or no opportunity at all – to verify the source of the funds flows. The FATF defines a payable-through account as a correspondent account that is used directly by third parties to transact business on their own behalf. Section 8(3)(e) of the Wwft refers to a situation where a bank in the Netherlands has a correspondent banking relationship with a foreign bank (in a non-Member State) and needs to ensure that, if that foreign bank gives its customers direct access to the account held with the bank in the Netherlands, the foreign bank has conducted equivalent customer due diligence on those customers and can provide relevant information about them to the bank in the Netherlands.

Additional information

- **The Wolfsberg Group, recommendations for correspondent banking,** http://www.wolfsberg-principles.com/pdf/home/Wolfsberg-Correspondent-Banking-Principles-2014.pdf

With respect 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.

4.8 Outsourcing

Pursuant to Section 10 of the Wwft, an institution may have the customer due diligence review carried out by a third party. An institution may outsource customer due diligence to identify the customer and the ultimate beneficial owner, a trust or a unincorporated partnerships to verify the identity of those persons and entities and to determine the purpose and envisaged nature of the business relationship.

Monitoring of the business relationship may, however, only be carried out by the institution itself.[21] However, for institutions governed by the Wft, where the third party is a member of the same group, such constant monitoring may be carried out by this party within the group.[22]

Ultimate responsibility for meeting the customer due diligence requirements remains with the institution that has outsourced the due diligence review. It is thus important that a judgment of the risk be made as to the expertise and practical approach of the third party in terms of compliance

[21] This is because Sections 3(2)(d), 3(3)(d) and 3(4)(e) of the Wwft are not referred to in Section 10 of the Wwft.

[22] Pursuant to Section 32 of the Bpr, the rules regarding outsourcing are not applicable to parties that are members of a group.

with the Wwft. In outsourcing it is important that the outsourcing institution not only lays down in writing that the third party will comply with all statutory requirements, but also that the institution should periodically check and verify this.

Outsourcing by trust offices

Trust offices can outsource activities to a third party on the basis of Section 9(4) Rib Wtt 2014.

5. MONITORING

5.1 General

During the customer acceptance process, the institution draws up a risk profile and expected transaction pattern of the customer. For the duration of the relationship it is important that the institution checks periodically whether the customer still fits his/her risk profile and whether the transaction pattern is in line with expectations. The institution may tailor the frequency and intensity of the reviews to the customer's risk classification. This is described in Section 4.2 of this Guidance.

In addition to periodically updating its customer data, the institution should also monitor customers' accounts and transactions. Monitoring allows the institution to gain and maintain an insight into the nature and background of customers and their financial conduct. Among other things, the purpose of this monitoring is to detect any changes in the transaction pattern and the possible occurrence of situations that present an enhanced risk. The institution pays particular attention to unusual transaction patterns and transactions which by their nature carry a higher risk of money laundering or financing of terrorism. The institution should check systematically whether there are any unusual or suspicious patterns or activities. For instance, transactions should be assessed to determine whether they are usual for the customer in question.

Examples of focus areas for monitoring

- Do the transactions serve an economic or commercial purpose?
- Are the amounts involved exceptionally large?
- Are the deposits, withdrawals or transfers out of proportion to the normal/expected business of the customer?
- Is the account and transaction activity in line with the activities of the customer?
- Are there transactions from and to countries with a heightened risk?

Monitoring of the relationship with the customer and of their transactions may be tailored to the type of relationship with the customer and their risk profile. This may vary per sector and per product. For instance, for life insurance products, annual checks could be conducted, e.g. when (annual) premiums are paid, and also when the contract or the beneficiary changes. If the policy establishes 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. For ordinary current accounts, the intensity of the monitoring effort might be lower than for (related) accounts of major international organisations.

Institutions are providing fewer and fewer teller services and are looking for alternatives to cash deposits. Where there is no direct contact with the customer, cash deposits may present a higher risk. Institutions should in such cases provide additional safeguards to ensure that the identity of persons using these alternatives is adequately determined and verified. Also, institutions should pay extra attention to alternative types of transactions to assess whether they match the customer's risk profile.

General recommendations for transaction monitoring:

- There should be a clear list of rules with relevant red flags and potential signals. It is advisable to use compound rules or transaction profiles to discover things such as 'smurfing' or 'rapid movements'.
- The monitoring includes all high-risk countries as identified by the FATF, UN, EU (such as sanctioned countries) and countries that appear on lists from other reliable and independent sources.
- There is a well-defined process for translating the rules into system parameters or (manual) queries, updating white lists, margins with batch tests, etc., possibly using a shadow system.
- The monitoring frequency is clearly set out and established in a risk-based way.
- Alerts are assessed in accordance with the described procedure (preferably involving the officer with responsibility for the customer and Compliance), in which an escalation pathway is also defined.

5.2 Monitoring money transfers: transaction analyses

As stated earlier, the institution should also monitor customers' transactions. In the case of money transfers, the institution will especially investigate the connection between particular transactions in order to identify unusual transactions (with an organised background). Institutions effecting money transfers should as a minimum analyse transactions using the method described below for the effective identification of unusual transactions.

Institutions effecting money transfers should periodically draw up lists of the top Dutch and foreign remitters and recipients for their investigation into the alleged misuse of money transfers. A top 10 for each category might suffice for small institutions, whereas for larger ones a top 50 would be more relevant. It is up to the institution itself to specify this in further detail. For the best result, analyses are effected on a monthly, quarterly or annual basis.

Depending on the outcome of the analyses, the institution should perform further customer due diligence, such as an investigation into the source and destination of funds.

Depending on the number of transactions and the risks identified, institutions conducting money transfers should carry out a supplementary review. Examples include:

- analyses in specific areas and/or countries (corridor reviews);
- transactions at addresses of Dutch customers (checking for actual existence and multiple use);
- transactions just below the reporting threshold ('smurfing');
- analyses per location (sales point).

Monitoring requirements for trust offices

Trust offices carry out continual checks of the business relationship pursuant to Section 10(1)(e), 4° of the Wtt in conjunction with Section 13(2)(d) of the Rib Wtt 2014. They use comparable methods for this to those described for other institutions. Services to object companies are subject to Section 19(1)(d) of the Rib Wtt 2014.

5.3 Monitoring methods

Monitoring may take place at various levels, depending on the risk and the extent of the activities. The higher the risk, the more intensive (in terms of frequency and depth) the monitoring effort should be.

Examples of monitoring methods

- **Spot checks:** targeted checks of accounts and transactions, e.g. of specific groups of customers, or of accounts and transactions earlier deemed to pose an enhanced risk on the basis of reports to FIU-NL or otherwise.
- **Manual monitoring:** the account manager knows his/her customers and their financial behaviour. Deviations from the customer's normal behaviour will immediately be spotted by the account manager. Key factors in this type of monitoring are an effective and realistic span of control as well as the expertise and competence of the persons carrying out the control operations.
- **Periodic management surveys/reports:** this type of monitoring is used in the case of fairly manageable numbers of customers and transactions. A daily, weekly or monthly printout of turnover, balance, exceeding of limits, fees charged and so forth may give an indication of which accounts require closer scrutiny.
- **Monitoring by hard indicators:** this method is used for an initial filtering on the basis of turnover, maximum balance, transaction amounts, countries of origin or destination, risk sectors, etc..
- **Intelligent transaction monitoring:** this type of monitoring is often based on the profiling of each account or customer. This profile may be made up of fixed rules concerning the turnover, transaction amounts, contra accounts, transaction frequency, transaction particulars, etc..
- **Behavioural monitoring:** in behavioural monitoring, the institution links transaction profiles to the customer's risk profile in order to detect potential money-laundering transactions. It should be possible using computer technology to expand and update profiles automatically based on old transactions, to reflect changes in current behaviour.

Several types of monitoring can be combined. For instance, monitoring combined with the profiling of payment and savings accounts with relatively low turnovers and balances will not be very interesting from a cost-versus-risk viewpoint. In contrast, hard indicators (turnover, maximum balance, transactions to and from specific countries and so forth) enable the institution to determine whether such an account should be reclassified from low risk to normal risk or even enhanced risk, after which intelligent monitoring could be applied. In monitoring, an institution will make a trade-off between cost, risk and the method to be used. For instance, manual monitoring could be in private banking operations, which fall in the high-risk category. An account manager knows his/her customers and will spot a change in financial activity without having to rely on intelligent monitoring systems. Once the number of customers per account manager becomes so large that the know-your-customer principle would suffer, other monitoring methods could be applied to ensure that the customer's financial activities are kept under surveillance.

Additional information

- **The Wolfsberg Group,** Monitoring Screening and Searching Wolfsberg Statement, http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Monitoring_Screening_Searching_Paper_(2009).pdf

5.4 Monitoring in high-risk jurisdictions

The FATF regularly identifies jurisdictions that have weaknesses in their anti-money laundering and counter-terrorist financing systems.[23] Maintaining business relationships with residents of these jurisdictions or conducting transactions to or from these jurisdictions might entail a higher risk of money laundering and terrorist financing, which could lead to the application of stricter measures. The FATF updates the list of jurisdictions, where appropriate, and DNB refers to these list on its website. As stated above, pursuant to Section 9 the Minister of Finance may also designate institutions to take further measures for customers that reside or are established or that have their registered office in certain designated states with strategic weaknesses in preventing money laundering and the financing of terrorism. The institution also applies these measures to transactions, business relationships and correspondent banking relationships related to those states. In addition to the FATF warnings and the 'mutual evaluation reports' from the FATF or the FATF Associate Members,[24] there are also other reliable sources indicating the degree to which international standards in relation to financial crime or terrorist activities are implemented by a country or jurisdiction. These sources may also prompt an institution to devote greater attention to business relationships and transactions involving people from those countries and jurisdictions. As part of their monitoring efforts, institutions will take the risks of money laundering and terrorist financing in specific countries into consideration.

Additional information

- **UN:** http://www.un.org/sc/committees/1267/index.shtml
- **IMF:** http://www.imf.org/external/ns/cs.aspx?id=175
- **FATF:** http://www.fatf-gafi.org/countries/
- **OECD:** http://www.oecd.org/corruption/

5.5 Assessment and record-keeping

If the institution has found transactions that do not fit the expected pattern or serve no economic or legal purpose, it will investigate the background and purpose of these transactions. The institution will pay particular attention to unusual transaction patterns and transactions which by their nature carry a higher risk of money laundering or financing of terrorism. The findings will be recorded in the customer file. If a transaction is suspected of being linked to money laundering or terrorist financing, it will be reported to FIU-NL. The considerations and decision-making as to whether or not to report a transaction should be laid down in writing by the institution.

[23] After each meeting, the FATF issues a public statement and a document called "Improving Global AML/CFT Compliance: ongoing process" in which it identifies jurisdictions which have weaknesses in their anti-money laundering and counter-terrorist financing systems.

[24] 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 on 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).

6. INFORMATION ACCOMPANYING WIRE TRANSFERS

FATF Special Recommendation VII[25] on wire transfers stipulates that electronic transfers must contain certain information about the party instructing the payment. In Europe, this FATF Recommendation has been transposed into Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds. The Regulation has direct effect in the Netherlands. The Wwft stipulates that a customer due diligence must be performed whenever an institution effects a non-recurring transaction into or out of the Netherlands on behalf of a customer or a trust that involves a transfer of funds as referred to in Section 2(7) of the Regulation. The Wwft also contains penalty provisions for non-compliance with this EC Regulation, and DNB has been charged with supervising compliance with this Regulation.

The Regulation lays down rules concerning the information on the payer that must accompany transfers of funds in order to ensure that the authorities responsible for combating money laundering and terrorist financing have direct access to basic information that can help them exercise their duties. Institutions will generally have access to this information from the customer due diligence. The institution also performs a customer due diligence when executing a non-recurring transaction into or out of the Netherlands on behalf of a customer or trust which is effecting a transfer of funds.

The term 'cover payment' refers specifically to international wire transfers where the instructing bank or institution has no direct relationship with the beneficiary bank or institution, and the transaction is effected through (several) correspondent or intermediary banks. Such payment transactions consist of two strands. One strand concerns the information from payer to payee and contains the customer information required under the EC Regulation. The other strand, i.e. the cover payment (SWIFT MT202COV), concerns the information exchange between the correspondent banks. Information on the payer also accompanies this cover payment, and the correspondent banks will ensure that all information received on the payer that accompanies a transfer of funds, will remain with the transfer. If SWIFT MT202 messages are used, the bank will be adequately controlling the risk of being used in a transaction between two unknown parties. Only bank-to-bank transactions would be allowed here, not an underlying transaction between two non-banks.

Full information about the payer consists of:

- Name
- Address (or date and place of birth, customer identification number or national identity number)
- Account number (if this is not available, replace it with a unique identification code that can be used to trace the payer).

Based on a risk assessment, the beneficiary institution should be particularly alert if information on the payer is lacking or is incomplete. If the required information on the payer is incomplete, the institution should reject the transfer or request full information on the payer. If an instructing institution regularly fails to provide the required information on the payer, the beneficiary institution should take measures, which may initially include issuing warnings and setting deadlines, before either rejecting any future transfers of funds from that institution or deciding whether or not to restrict or terminate its business relationship with that institution. The beneficiary institution should report this fact to FIU-NL.

Additional information

- **EU,** http://ec.europa.eu/internal_market/payments/transfers/index_en.htm
- **3L3 Anti-money laundering and terrorism financing group (3L3 AMLTF),** http://www.c-ebs.org/documents/10180/16166/2008+16+10+AMLTF+Common+understanding+on+payment+funds+transfer.pdf
- **BCBS / ILG Anti-money laundering and terrorism financing Expert Group (AMLEG):** http://www.bis.org/publ/bcbs154.htm

[25] During the review of the FATF Recommendations in 2012, FATF Special Recommendation VII was changed to Recommendation 16. This change has not yet been incorporated into the EU Regulation.

7. RECORD-KEEPING AND DATA RETENTION OBLIGATION

Several laws[26] stipulate that institutions must retain customer and transaction data. This concerns all data obtained during the customer due diligence process, e.g. copies of identity documents, account particulars, correspondence, memos of conversations about and with the customer, transactions effected by and other services provided to that customer. The customer file should also reveal how the decision-making process surrounding customer acceptance has taken place, e.g. in the case of high-risk customers.

For legal entities, records should include the particulars of the natural persons representing the legal entity vis-à-vis the institution. For the ultimate beneficial owner, the person's identity and the method by which it was verified should be recorded. If a customer acts as a trustee, the institution also records data in a retrievable manner concerning the founders, trustees and ultimate beneficial owners. Where a customer acts as partner in an unincorporated partnership, the institution should record the particulars of all partners, the persons authorised with respect to the management of the unincorporated partnership and the persons who are able to exert considerable influence on or have considerable interests in the partnership.

Data retention obligation

- Institutions must retain these data for at least five years following termination of the business relationship or following the provision of services.
- In the case of a non-recurring transaction, the period of data retention should be at least five years after the transaction was carried out.

The purpose of the data retention obligation is to enable the authorities to gain an understanding of a customer's activities, e.g. in the event of a (criminal) investigation. The various records and files should therefore be easily accessible to the supervisory authorities. It makes no difference whether the data are stored electronically or as a physical document.

Requirements for trust offices

It follows from Section 25(3) of the Rib Wtt 2014 that trust offices, with due observance of applicable legal requirements, must retain a customer acceptance file for a period of at least five years after the end of the provision of services.

The Guidelines 'Identification and verification of personal data' of the Dutch Data Protection Agency (*College Bescherming persoonsgegevens,* CBP) state that a financial institution – as proof of the identification requirement (duty to reproduce) – can document a copy of the verified identity document. On the basis of the Wwft, Section 33, there is no requirement to document the citizen service number (*burgerservicenummer,* BSN)

[26] Section 33 of the Wwft, Section 14 of the Bpr, Section 10, Book 2 of the Netherlands Civil Code (*Burgerlijk Wetboek* / BW), Section 52 of the State Taxes Act (*Algemene Wet inzake Rijksbelastingen* / AWR)

8. REPORTING UNUSUAL TRANSACTIONS

Institutions are obliged to report unusual transactions to FIU-NL. A list of indicators is used to assess whether a transaction is unusual.

8.1 Reporting duty

Section 16 of the Wwft requires institutions to report an actual or intended unusual transaction. The Appendix to Section 4 of the Decree containing provisions on the scope of the Wwft (*Uitvoeringsbesluit Wwft*) contains a list of indicators based on which a report must be submitted. This list can be used to assess whether a transaction should be classified as an unusual transaction. The indicators are subdivided into objective and subjective indicators. The objective indicators describe situations in which transactions must always be reported. The Appendix to the Decree 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 lies on the subjective indicator. The subjective indicator forces 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 under the scope of the Wwft. The institution will consider whether a particular transaction needs to 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.

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 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 in the course of providing services to that customer. It is not a requirement that there must be a direct or causal connection between the unusual transaction and the activities of the institution. The words '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.

Processes for detecting unusual transactions

- Clear internal indicators or ‘red flags’ have been identified that can help employees decide whether a transaction is unusual.
- The indicators focus on unusual transaction patterns, deviating behaviour on the part of the customer, and activities that are illogical based on knowledge of the customer or sector.
- The front and/or mid-office is responsible for detecting potentially unusual transactions, services or products.
- Compliance is involved in assessing a possible unusual transaction and is responsible for reporting to FIU-NL.

In addition to the indicators, the 'gut feeling' of employees is also important.

The annual summaries of FIU-NL contain examples of money laundering. Case studies are also regularly published on the FIU-NL website.
http://www.fiu-nederland.nl/content/jaaroverzicht
http://www.fiu-nederland.nl/casuistiek

8.1.1 Life insurers

The general perception is that life insurance is often a low-risk standard product. This view is reinforced by the fact that insurers do not deal with cash and that the funds flows go through banks. However, it is likely that banks are less thorough in their scrutiny of payments to and from life insurers, because they involve transactions with institutions that are also governed by the Wwft. Besides, banks do not have insight into the underlying insurance contracts.

The examples below are examples of indicators of transactions that can be a reason for a life insurer to further examine the transaction and to assess if these are factors to determine the transaction as an unusual transaction. A number of those transactions will already be notice in the primary work process. For other indicators, the life insurer will regularly have to run queries to test if transactions were possibly unusual.

Examples for life insurers of indicators pointing to possible unusual transactions. These indicators do not refer to amounts as these will be based on a life insurer's own analysis.

- Policies with an initial high deposit or a high additional payment on the policy.
- Payments of premiums originating in a country designated as high-risk.
- Policyholder, beneficiary or premium payer resident or located in the Netherlands moves to a country designated as a high-risk country.
- Surrendered (single or periodic payment) policies running under 3 years with a surrendered value of over [€ xx] *and* a surrendered value equals 50% or more of paid-up premiums.
- Policyholder, beneficiary or premium payer is a foreign legal entity or a natural person resident or located outside the Netherlands.
- Annual payments totalling over [€ xx] to high-risk countries.
- One-off pay-outs of [€ xx] or more.
- Regular pay-outs of [€ xx] or more on an annual basis.
- Premium payback on single payment 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 home mortgage lending.

Additional information

- **FATF,** typology report, FATF Money Laundering and Terrorist Financing 2004-2005, http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf
- **IAIS,** examples (October 2004), http://www.iaisweb.org/view/element_href.cfm?src=1/209.pdf
- **IAIS**, Application Paper on Combating Money Laundering and Terrorist Financing, October 2013, http://iaisweb.org/index.cfm?event=openFile&nodeId=34107

8.1.2 Trust offices

It should be noted when reading the following examples for trust offices that the Wwft adopts a very broad definition of the term 'transaction', and that if a trust office does not execute the transaction, or does not accept a customer because of these types of transactions, that transaction will be reported to FIU-NL as an intended unusual transaction.

Examples of transactions relating to legal entities and structures that warrants extra attention from a trust office:

- The customer uses or wishes to use one or more intermediate foreign or acquired legal persons or companies without there being or appearing to be plausible tax, legal or commercial reasons to do so.
- The customer wishes to incorporate several legal persons or companies within a short period of time on behalf of another person, without there being or appearing to be plausible tax, legal or commercial reasons to do so.
- The customer wishes to incorporate or acquire a legal person or company with a doubtful (envisaged) object or an object that does not appear to bear a relationship to its normal professional, business or other activities, or with an object whose performance requires a licence, whereas the customer has no intention of obtaining such a licence and is unable to give the institution an acceptable explanation for this.
- The customer makes use of legal persons or companies in which the control structure is not transparent or which, because of their nature or method of incorporation, are suitable for masking the identity of the underlying beneficial owner (e.g. bearer shares, trusts, foreign legal persons), without being able to give the institution an acceptable explanation for this.
- The frequent alteration of legal structures and/or changing of directors of legal persons or companies. There is a complex legal structure that does not appear to serve a genuine object.

Additional information

- **FATF**, typology report, Money Laundering Using Trust and Company Service Providers, October 2010, http://www.fatf-gafi.org/documents/documents/moneylaunderingusingtrustandcompanyserviceproviders.html

8.1.3 Credit cards

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

Examples of indicators pointing to possible unusual transactions of credit card transactions.

Funding of the card

- Cash payments into a current account, the purpose of which is to pay for credit card expenditure
- Funding by a third party (not being the card-holder) 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 cards or stored value cards (vouchers)
- 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 card-holders with particular merchants (purchase of luxury products)
- Making structured use of stolen credit cards at E-commerce merchants

Other signals

- Problems with identification and/or verification (applicant and/or ultimate beneficial owner)
- Dependence of merchant on certain card-holders due to turnover (volume)
- Relationships between card-holder(s) and merchant(s) (criminal organisation and anonymous use)
- Forgery
- Cybercrime (including phishing, skimming and use of malware)

8.1.4 Reporting procedure

An inherent part of the reporting duty is that institutions have in place processes and procedures to recognise and report the unusual nature of transactions. In addition, pursuant to Section 32 of the *Wwft*, the supervisory authorities may instruct an institution to develop internal procedures and controls to prevent money laundering and terrorist financing, if the institution fails to meet the requirement to report unusual transactions. There are also requirements based on other financial supervision legislation, which necessitate institutions to have procedures and measures in place to control integrity risks. As mentioned earlier, the letter from the Minister of Finance to the Dutch Parliament dated 15 October 2008 (Parliamentary Paper 31237, No. 9) states that the procedures used for the implementation of the Wft and the Wwft can be integrated so that the requirements under the two Acts can be met in the same manner.

The (intended) unusual transactions are reported to FIU-NL immediately after their unusual nature has been identified. Furthermore, as also stated in the list of indicators (see Section 8.1), where transactions are reported to the police or the Public Prosecution Service in connection with suspected money laundering or terrorist financing, it is appropriate that they should also be reported to FIU-NL, given that there is a suspicion of money laundering or terrorist financing.

Based on European case law, it has been determined that the FIU must be able to request information in relation to money laundering and terrorist financing from institutions that operate in a country without having a physical presence in that country, and that transactions must therefore also be reported to the FIU in the country where the activities take place. This enables supervision to be exercised of all financial transactions performed by institutions within a Member State, regardless of the way in which those institutions offer their services.[27]

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 authorities, 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.

8.2 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.

The civil indemnification means that an institution cannot be held liable under civil law for the loss suffered by another party (the customer or a third party) as a result of a report as long as the institution acted on the reasonable assumption that it was implementing the 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, to claim 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 in good faith and correctly in accordance with the requirements of the Wwft.

8.3 Confidentiality

The Wwft imposes a strict duty of confidentiality. This means that institutions are obliged to observe confidentiality in respect of an unusual transaction report. Exceptions are possible in so far as they arise from the law. Put briefly, these exceptions to the obligation of confidentiality permit the institution to exchange information with units of its own organisation or network elsewhere and/or 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. Although, under Section 28 of Directive 2005/60/EC, the obligation of confidentiality is not only to apply to customers but also to third parties, it cannot be the intention of this Directive to obstruct these

[27] Ruling by the European Court of Justice in the case of Jyske Bank Gibraltar Ltd v Administración del Estado, C-212/11, 25 April 2013.

systems, which help prevent the financial system from being misused for money laundering or terrorist financing purposes.[28]

[28] Section 23(5) of the Wwft.

9. SANCTION REGULATIONS

9.1 Introduction

The General Guidance of 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 (SW) and its reporting procedure.

The AFM and DNB have been charged with the supervision of compliance with the SW with respect to financial transactions. To that end, the two supervisory authorities have jointly adopted the Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling Toezicht Sanctiewet 1977*). This Regulation prescribes that an institution must take measures to verify whether relationships of the institution appear on one or more sanction lists (such as EU decisions and/or regulations, decisions by 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'[29]- or UN Security Council Resolutions). The European Union Regulations describe several financial sanctions:

- an order to freeze funds and assets of designated persons or organisations;
- a ban on making resources available to these persons or organisations directly or indirectly;
- a ban or restrictions on providing financial services.

Institutions must at all times be in a position to find out whether their relationships or transactions appear in, or their services relate to, the sanction regulations. Institutions must also (be able to) inform DNB of this immediately. This requirement cannot be met using a risk-based approach (in other words, the institution cannot choose whether or not to implement the sanction regulations). The way in which a transaction or relationships is assessed in relation to the sanction regulations (e.g. manually or electronically) and the frequency of this assessment can however be carried out using a risk-based approach. [30] This means that explicit attention must also be devoted during the risk assessment to the necessary frequency of the periodic screening against the sanction lists.

9.2 Administrative organisation and internal control

AFM and DNB, in their capacity as the supervisory authorities, assess and enforce 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 align with existing rules regarding administrative organisation and internal control (AO/IC) that arise from other regulations such as the Wft or the Wwft. The basic principle for the implementation of the AO/IC by financial institutions is that they should act in line with the objectives of the sanctions regulations. Put briefly, this means that institutions are able to check their records in such a way that legal and natural persons and entities (and their financial assets) that are named in the sanctions regulations can be detected. It must be possible to freeze the financial assets immediately and/or to prevent financial assets and/or services being made available to these legal/natural persons and entities. It is not permitted to exit an existing client and in some cases an exemption by be requested from the ministry of Finance. If the institution establishes that a relationships' identity corresponds with that of a natural or legal person or entity as referred to in the sanctions regulations (a 'hit'[31]), the institution must report this immediately to the supervisory authorities using the prescribed report form. These are matches between the names and other identification data, such as date and place of birth and place of residence.

[29] See for the Dutch list of persons and organisations with frozen assets, http://www.rijksoverheid.nl/onderwerpen/internationale-sancties/documenten-en-publicaties/rapporten/2014/08/15/personen-en-organisaties-met-bevroren-tegoeden.html, per 13-01-2015

[30] Zie Chapter 3 for guidance on the integrity risk analysis.

[31] An institution will encounter many potential hits when screening against the sanction lists. These are all checked for correspondence with the various lists. Only genuine hits are reported; 'false positives' are not.

9.3 Relationships

The concept 'relationship'
The Regulations adopt a broad definition of the term 'relationship', namely anyone involved in a financial service or financial transaction. This includes:

- customers
- representatives or authorised agents
- ultimate beneficial owners of customers
- beneficiaries of a product (e.g. life insurance payments) or (international) transfers of funds
- counterparty to a financial transaction/product (e.g. non-life insurance payments)
- person(s) involved in a financial transaction where the party to the transaction is a company receiving services from a trust office

The term 'relationship' is defined so broadly because both the direct and indirect provision of financial resources or services fall 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 clarify that providing funds to persons or entities that were not on the sanction lists but were under the control or ownership of persons or entities that do appear on the sanction lists, should in principle be regarded as the indirect provision of funds to the sanctioned person or entity.[32]

It qualifies as indirect provision, in case a person has 50% or more ownership in a structure or in case a person has control (whereby control very broadly is defined in the Guidelines) is exercised,. If the person who holds 50% or more or property rights or who exercises control is listed on a sanctions list, the assets of the legal entity must be frozen also and the entity should be prevented from receiving funds. In practice, institutions can also register UBOs with less than 50% ownership. Thus it is recommended that institutions apply the definition of an ultimate beneficial owner (*uiteindelijk belanghebbende*) set out in the Wwft, and therefore ascertain the identity of all UBOs holding 25% or more of property rights. Indeed, it is forbidden to provide funds to persons or entities that are under control of a sanctioned person. And for control there is no requirement to hold 50% of more of the shares.

Where only part of a customer is listed, the institution should in order to comply with the sanctions regulation , for the other, non-listed part identify the ultimate beneficial owner.

During the customer acceptance process, all relevant relationships are defined and recorded in the relationship file. As well as the customer, this also includes other persons and entities that are involved with the financial service or transaction, such as the customer's ultimate beneficial owner(s), representatives, authorised agents and beneficiaries (where known). Since the term 'relationship' is so broadly defined, an institution charting all relationships can include persons depending on whether they own or control or can obtain control of the funds.

During the identification process, information is recorded such as the name, date of birth, place of residence and address of establishment of these persons and entities. This information enables the institution to perform proper checks. The absence of a date of birth or address, for example, can make it more difficult to assess a hit. For legal persons, it is generally sufficient to carry out a check of the information contained in the Trade Register at the Chamber of Commerce, while for natural persons checking (a copy of) their passport is usually sufficient to enable adequate screening against the sanction regulations. When identifying ultimate beneficial owners, it is not always necessary to record the intervening layers in the group structure. It is enough to record the information on the UBO by carrying out a check on the Trade Register or (a copy of) the UBO's passport.

If the institution is aware of changed relationships with regard to a customer, it must update its relationship file. With regard to relationships qualifying as high-risk (e.g. relationships that deal with countries on sanction lists), the institution is expected to play a more active role in identifying changes in its relationship file, for example by periodically enquiring whether there have been any

[32] Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy - new elements, 9068/13, http://register.consilium.europa.eu/pdf/en/13/st09/st09068.en13.pdf

changes in the relevant relationships. The complete relationship file should then be screened against all sanction lists and sanction regulations, both on acceptance and periodically thereafter. The periodic screening can be carried out using a risk-based approach.

The institution should 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 should record all this information in an accessible way.

9.4 Filtering of transactions

In principle, the parties involved in a financial transaction are screened against the sanction lists. If these parties are already known to the institution and the institution checks the relationship file on acceptance and sufficiently frequently thereafter, screening against the sanction lists in the event of payments is not necessary. Institutions can also be confident that funds will be frozen where necessary if there are adequate safeguards and/or agreements between the institutions involved in a transaction that the sanction regulations will be properly observed by both sides. As part of these agreements, it would be logical that institutions inform each other of transactions that are blocked. If institutions make agreements in this regard, they should be aware that, when making agreements with an institution abroad, the Dutch sanction list will generally not be checked. The institution ensures that its AO/IC is configured such that the objectives of the sanction regulations are also met in the event of payments to third parties.

How can an institution filter transactions against sanction lists?

- Information or fields against which checks are carried out as a minimum:
  - ordering party
  - beneficiary
  - place names
  - country
  - description
- The institution filters the SWIFT MT series and fields (including the n99 messages) or SEPA messages and field that it has identified on the basis of a documented risk assessment.
- Trust offices, insurers and institutions with limited payment transactions carry out a check when making payments to third parties/beneficiaries as to whether the legal or natural person concerned appears on the sanction lists.

9.5 Reporting to DNB

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

- Identifying information (name, alias, address, place and date of birth)
- the amount and nature of the funds or assets frozen
- the action taken by the institution
- the number of the applicable sanction regulation

Institutions use the report format drawn up by AFM and DNB to report a hit to the relevant supervisory authority.[33] DNB assesses the reports received from financial institutions. In the event of a genuine hit, DNB forwards the report to the Ministry of Finance. If DNB believes, in assessing the report, that it is not a hit the report is not forwarded to the Ministry of Finance. In both cases the reporting institution is advised accordingly.

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

Liability insurance is a special case in this regard. 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, if it transpires, when checking, that the beneficiary appears on the sanction lists, the insurer is forced to freeze the funds on the grounds of the sanction regulations, whereas on the grounds of other regulations the insurer may have an

[33] http://www.toezicht.dnb.nl/en/2/51-221960.jsp

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 Ministry of Finance. Based on a substantiated request for exemption, the Minister may 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.

Meanwhile, it appears only to be expected that where an institution freezes assets on the basis of a match with the 'terrorist lists', it will also look at the owner's transaction history to see whether any transactions have occurred that warrant the conclusion that they may have been made in connection with terrorist financing. In case of a suspicion of terrorism financing, the institution will report those transactions to the FIU in accordance with the Wwft.

Assets should remain frozen until the relevant sanctions regulation is changed and the obligation to freeze the assets is lifted, an exemption is granted or if otherwise notice to the contrary is received from the Ministry of Finance or the supervisory authorities. If the institution does not hear anything, it should assume that the assets are to be considered an actual 'hit' and should remain frozen until further notice.

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

Additional information

- **Rijksoverheid**, http://www.rijksoverheid.nl/onderwerpen/internationale-sancties
- **DNB,** information on the sanction regulation, http://www.toezicht.dnb.nl/4/6/50-204700.jsp
- **DNB,** Q&A Naleving Sanctiewet 1977 binnen SEPA, http://www.toezicht.dnb.nl/en/3/51-230317.jsp

10. TRAINING

To ensure adequate implementation by institutions of the processes and procedures pursuant to the Wwft and the SW, the degree of experience and knowledge of their employees is of paramount significance. This means that adequate knowledge and experience on the part of employees concerning the management of the risks of money laundering and terrorist financing are important prerequisites for an adequate control framework. Training of employees is an important tool to communicate and anchor knowledge within the institution about the Wwft and the SW and about the principles and procedures of the integrity policy.

Institutions should provide training programmes to create awareness among their employees about the provisions of the Wwft and the SW, thereby enabling them to carry out customer due diligence adequately and fully, and to identify unusual transactions. These programmes should focus on money laundering and terrorist financing techniques, methods and trends, on the international context and standards, and on new developments in this area. To keep abreast of new developments and to promote permanent awareness, this training will usually not be a one-off occasion, but will be provided regularly and at different levels.

It is logical for members of the Compliance department to take additional training courses to learn about developments in relation to national and international legislation and regulations, and the risks of money laundering and terrorist financing.