# Consultatieversie DNB 'Q&As' en 'Good Practices' Wwft

DeNederlandscheBank

EUROSYSTEEM

# Inhoud

Inleiding

Kader

Cliëntenonderzoek: cliëntacceptatie

Cliëntenonderzoek: voortdurende controle

Bijlage I – Afkortingenlijst

# 1 Inleiding

Integriteit is – naast soliditeit – een voorwaarde voor een gezond financieel stelsel. De Nederlandsche Bank (DNB) houdt integriteittoezicht op een breed scala aan (financiële) instellingen. Onderdeel hiervan is onder meer het voorkomen van het gebruik van het financiële stelsel voor witwassen en financieren van terrorisme. Het kader hiervoor staat hoofdzakelijk beschreven in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). De Wwft is de implementatie van de Europese richtlijn ter voorkoming van witwassen en terrorismefinanciering (AMLD).[1]
Deze Europese richtlijn is mede gebaseerd op de aanbevelingen van de Financial Action Task Force (FATF). Het door DNB gehouden integriteittoezicht is, naast de Wwft, gebaseerd op de Wet op het financieel toezicht (Wft), Pensioenwet, de Wet toezicht trustkantoren 2018 (Wtt 2018) en de Sanctiewet 1977 (Sw).[2]

Met deze 'Q&As' en Good Practices Wwft' (hierna: Q&As/Good Practices) beoogt DNB een handreiking te doen voor de uitleg en toepassing van de wettelijke verplichtingen omtrent het voorkomen van witwassen en financieren van terrorisme. Deze Q&A's/Good Practices vervangen de door DNB eerder gepubliceerde DNB Leidraad Wwft & Sw. Dit document richt zich enkel op de regels omtrent het voorkomen van witwassen en financieren van terrorisme zoals met name neergelegd in de Wwft.[3]
Het toezicht op de naleving van de Wwft is toebedeeld aan DNB voor wat betreft de volgende typen instellingen: banken, levensverzekeraars, betaaldienstverleners en -agenten, elektronischgeld-instellingen, aanbieders van cryptodiensten,[4] wisselinstellingen, trustkantoren,[5] andere financiële ondernemingen,[6] en bepaalde bijkantoren.[7] Daarmee gelden voor trustkantoren aanvullende eisen waar dit document geen nadere aandacht aan besteedt.[8]

**Status Q&As**

Door DNB uitgevaardigde Q&As geven aan hoe DNB naar de invulling en toepassing van wettelijke normen kijkt. Q&As vormen dus een interpretatie van die normen. Instellingen kunnen daarom ook op andere wijze aan de wet- of regelgeving voldoen. Instellingen moeten daarbij wel gemotiveerd kunnen aantonen dat zij met hun invulling voldoen aan de wet- of regelgeving. Voor een nadere toelichting op de status van de beleidsuitingen van DNB zie de Leeswijzer beleidsuitingen DNB op Open Boek Toezicht.

1 Richtlijn 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie, PbEU 2015, L 141/73, zoals nadien gewijzigd
2 Daarnaast houdt DNB integriteittoezicht op instellingen in Caribisch Nederland. Voor dit geldt een eigen wet- en regelgeving.
3 Het deel over de Sanctiewet dat in de huidige DNB Leidraad Wwft & Sw staat, zal in afwachting op het nieuw wettelijk kader, opnieuw worden gepubliceerd in een afzonderlijk document.
4 Zoals bedoeld in art. 1a lid 4 onder l en m Wwft.
5 Voor trustkantoren geldt in het bijzonder ook de Wtt 2018. Daarmee gelden voor trustkantoren aanvullende eisen waar dit document geen nadere aandacht aan besteedt.
6 Andere financiële ondernemingen als bedoeld in art. 1a lid 3 onder a Wwft. De Wwft verwijst naar degenen die, geen bank zijnde, in hoofdzaak hun bedrijf maken van het verrichten van een of meer van de werkzaamheden opgenomen onder de punten 2, 3, 5, 6, 9, 10, 12 en 14 van bijlage I bij de richtlijn kapitaalvereisten.
7 Dit betreft bijkantoren in Nederland van banken, betaaldienstverleners, elektronischgeldinstellingen, wisselinstellingen, levensverzekeraars en andere financiële ondernemingen zoals bedoeld in art. 1a lid 3 onder a Wwft.
8 De Good Practices voor de trustsector worden momenteel herzien.

**Status Good Practices**
Good Practices bevatten suggesties of aanbevelingen voor instellingen. Het zijn voorbeelden van mogelijke toepassingen die naar het oordeel van DNB goede invulling kunnen geven aan de verplichtingen uit wet- en regelgeving. Instellingen zijn vrij om een andere toepassing te kiezen, zolang men anderszins voldoet aan de wet- en regelgeving en dit gemotiveerd kan aantonen. Voor een nadere toelichting op de status van de beleidsuitingen van DNB zie de Leeswijzer beleidsuitingen DNB op Open Boek Toezicht.

**Van herstel naar balans**
Met deze Q&As/Good Practices geeft DNB ook een vervolg aan het op de banksector gerichte rapport 'Van herstel naar balans'.[9]

In dit rapport bepleit DNB dat het tegengaan van financieel-economische criminaliteit efficiënter en effectiever kan door een meer risicogebaseerde aanpak van instellingen én toezichthouders.
Door slimmere toepassing van datagedreven technologische innovaties. Door een meer gerichte samenwerking in de hele keten. Waarbij niet angst om het fout te doen de boventoon voert, maar het vertrouwen dat we in Nederland financieel-economische criminaliteit zoveel mogelijk tegengaan als we er met alle betrokkenen de schouders onder zetten.[10]
Een effectievere aanpak betekent primair dat er minder criminele gelden door de financiële infrastructuur gaan. Dit zal tot uiting komen in het vaker weren van criminelen aan de poort. En waar crimineel geld toch het systeem in komt in betere detectie, meer veroordelingen en meer afgepakte gelden. Een efficiëntere manier om financieel-economische criminaliteit tegen te gaan betekent een beperktere belasting van instellingen én hun klanten waar dat kan. Een effectievere en efficiëntere aanpak kan worden gerealiseerd door een meer risicogebaseerde aanpak door instellingen én toezichthouders.

Deze Q&As/Good Practices benadrukt het doel van de Wwft, namelijk dat poortwachters voorkomen dat het financiële stelsel wordt gebruikt voor witwassen en financieren van terrorisme.
De maatregelen die instellingen in het kader van de Wwft nemen, dienen bij te dragen aan dat doel – en zijn daarmee in beginsel geen doel op zich. De Wwft legt ook verplichtingen op aan instellingen waarin geen ruimte bestaat voor een risicogebaseerde aanpak. Aan die verplichtingen moeten instellingen zich onverkort houden.

9 DNB (2022), 'Van herstel naar balans. Een vooruitblik naar een meer risicogebaseerde aanpak van het voorkomen en bestrijden van witwassen en terrorismefinanciering, www.dnb.nl/media/2ambmvxt/van-herstel-naar-balans.pdf.
10 DNB, (2022), Van herstel naar balans. Een vooruitblik naar een meer risicogebaseerde aanpak van het voorkomen en bestrijden van witwassen en terrorismefinanciering, p. 3.

**Leeswijzer**

De Q&As/Good Practices is als volgt opgebouwd:

| Hoofdstuk | Titel | Toelichting |
|---|---|---|
| 1 | Inleiding | |
| 2 | Kader | Dit hoofdstuk gaat in op het kader waarbinnen de naleving van de Wwft binnen een instelling tot stand komt. De cyclus van risicomanagement c.q. de compliance cycle staat hierin centraal. Daarnaast komen uitbesteding, de verplichtingen uit de Wire Transfer Regulation (WTR2), het melden van misstanden en de bescherming van persoonsgegevens aan de orde. |
| 3 | Cliëntenonderzoek: cliëntacceptatie | Dit hoofdstuk gaat in op het proces van cliëntacceptatie dat een instelling op grond van de Wwft doorloopt. De verschillende onderdelen van het cliëntenonderzoek, zoals de identificatie en verificatie van de cliënt en de UBO en het onderzoek naar de bron van de middelen, worden behandeld. Ook gaat dit hoofdstuk in op situaties van hoger en lager risico. |
| 4 | Cliëntenonderzoek: voortdurende controle | Dit hoofdstuk kent twee onderdelen wat betreft de voortdurende controle, namelijk transactiemonitoring en de review van de cliënt. |
| Bijlage 1 | Afkortingen | Deze bijlage bevat een lijst met veelgebruikte afkortingen. |

# 2 Kader

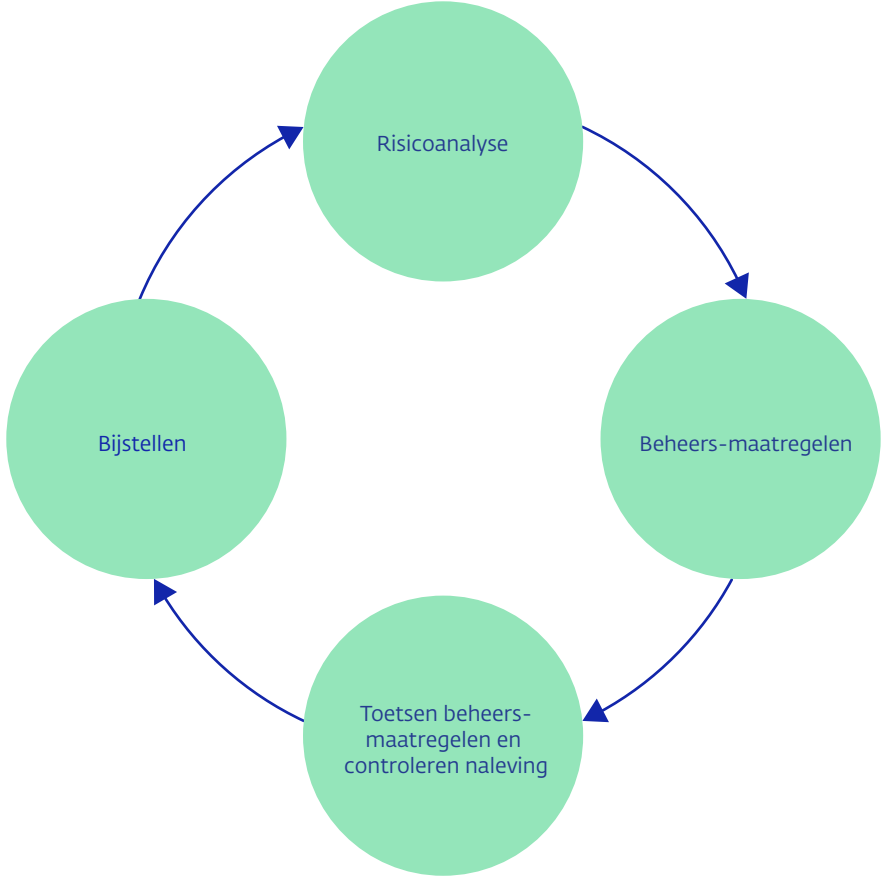
## 2.1 Risicobeheersing en bedrijfsvoering

Het doel van de Wwft is, zoals de naam al uitdrukt, het voorkomen van witwassen en financieren van terrorisme. Daarbij kent de wet een risicogebaseerde benadering.[11] Het gaat erom dat de instelling haar risico's op betrokkenheid bij witwassen en financieren van terrorisme afdoende beheerst en met het oog daarop passende maatregelen neemt.

De intensiteit van de maatregelen ter voorkoming van witwassen en financieren van terrorisme dient waar mogelijk te worden afgestemd op de concrete risico's. Zo zullen cliënten met verhoogd risico meer aandacht moeten krijgen, terwijl bij cliënten met een geringer risico kan worden volstaan met een minder intensieve controle.

Bij de risicogebaseerde benadering vormt de risicoanalyse het uitgangspunt. Op basis hiervan kan de instelling passende beheersmaatregelen vaststellen. Daarbij is het ook van belang dat de instelling de naleving en effectieve werking hiervan toetst, en waar nodig bijstellingen doet. De systematiek die uit de Wwft volgt ten aanzien van het voeren van een risicogebaseerd beleid, kan als volgt worden weergegeven:

In de uitvoering van haar toezichthoudende taak toetst DNB de naleving van de Wwft. Hierbij wordt de gehele systematiek beoordeeld.




11 Kamerstukken II 2017-2018, 34 808, nr. 3, p. 8.

### 2.1.1 Risicoanalyse

Een solide risicoanalyse is cruciaal in het voorkomen van financieel-economische criminaliteit. De risicoanalyse brengt de belangrijkste integriteitsrisico's in kaart waaraan een instelling is blootgesteld als gevolg van haar bedrijfsvoering. Een instelling die goed inzicht heeft in haar integriteitsrisico's, zowel op het niveau van de eigen organisatie als op het niveau van de cliënt, kan haar aanpak daarop aanpassen.[12] Sterker: zonder een goede risicoanalyse is de juistheid van de beheersmaatregelen voor de betrokken bedrijfsvoering niet vast te stellen.

De analyse waarin risico's op witwassen en terrorismefinanciering worden vastgesteld en beoordeeld, is een sturingsdocument voor het management.

- De risicoanalyse biedt inzicht in waar de gepercipieerde integriteitsrisico's voor de instelling in kwestie het grootste zijn (toprisico's).
- Op basis van deze analyse bepaalt de instelling vervolgens waar de belangrijkste prioriteiten liggen en welke acties de instelling daarop zou moeten initiëren om deze risico's te mitigeren.

Dit betekent ook dat de risicoanalyse het uitgangspunt is voor het opstellen van beleid, bestaande uit procedures en maatregelen, om geïdentificeerde risico's te beperken en effectief te beheersen. De naleving van dit beleid wordt gecontroleerd door de compliancefunctie. Ook de intensiteit van de invulling van de auditfunctie wordt afgestemd op de risicoanalyse.[13]

#### Q&A

**QA.2.1: Vraag**

Hoe past de risicoanalyse van de Wwft in de risicoanalyse van de SIRA?

**Antwoord**

SIRA staat voor systematische integriteitsrisicoanalyse. In onder meer het Besluit prudentiële regels Wft (Bpr) is bepaald dat instellingen zorgdragen voor een systematische analyse van integriteitsrisico's.[14] De risicoanalyse in de Wwft richt zich op de blootstelling van een instelling aan het risico op witwassen en financieren van terrorisme, terwijl de systematische integriteitsrisicoanalyse een breder bereik heeft. Het ligt voor de hand, hoewel niet verplicht, dat de risicoanalyse uit hoofde van de Wwft onderdeel is van de SIRA als de instelling tevens verplicht is om een SIRA op te stellen.[15]

---

**QA.2.2: Vraag**

Wat houdt een risicoanalyse in?

**Antwoord**

Risico's zijn verbonden aan het bedrijf dat de instelling uitoefent. Dit betekent dat een risicoanalyse allereerst specifiek is voor de instelling en met name aandacht heeft voor de risico's die verbonden zijn aan de eigen bedrijfsvoering.

De risico's met betrekking tot witwassen en financieren van terrorisme kunnen nader in kaart gebracht worden door onder meer een goede analyse te doen van de risico's in de cliëntenportefeuille,

12 Art. 2b Wwft; Art. 2c lid 1, 2 Wwft.
13 Kamerstukken II 2017-2018, 34 808, nr. 3, p. 8, 43-45.
14 Art. 10 lid 1 Bpr.
15 Kamerstukken II 2017-2018, 34 808, nr. 3, p. 43.

en door na te gaan hoe de risico's de instelling kunnen raken en wat daarvan de (negatieve) gevolgen zouden zijn. Negatieve gevolgen betreffen bijvoorbeeld de 'besmetting' van het financiële stelsel met criminele gelden dan wel de doorvoer van gelden waardoor terroristische activiteiten gefinancierd worden.

Hierna kan bepaald worden welke beheersmaatregelen dit voldoende tegengaan.

Zie voor nadere guidance en handvatten de SIRA Good Practice van DNB.[16] De methode om een SIRA te ontwikkelen is ook toepasbaar op de risicoanalyse voor witwassen en financieren van terrorisme.

**QA.2.3: Vraag**

Met welke risicofactoren dient een risicoanalyse rekening te houden?

**Antwoord**

De risicofactoren, indicatoren die duiden dat een risico zou kunnen spelen, zijn afhankelijk van het profiel en de dienstverlening van de instelling. Bij het vaststellen en beoordelen van de risico's waar de Wwft op ziet, houdt de instelling in ieder geval rekening met de risicofactoren die verband houden met het type cliënt, product, dienst, transactie en leveringskanaal en met landen of geografische gebieden.[17]

Er is een onderscheid in het niveau waarop risico's ten aanzien van witwassen en financieren van terrorisme zich voordoen:

- Op het niveau van de Europese Unie is de supranationale risicobeoordeling beschikbaar.[18]
- Op nationaal niveau is de nationale risicobeoordeling beschikbaar.[19]
- De instelling beschikt over een risicoanalyse op het niveau van de instelling[20] Daarbij houdt de instelling in ieder geval rekening met de risico's die verbonden zijn aan type cliënten, producten, diensten, transacties, leveringskanalen en met landen of geografische gebieden.[21]

Ook binnen een individueel cliëntenonderzoek houdt een instelling rekening met risico's die zich in dat geval voordoen. De instelling stemt cliëntenonderzoeken af op de risicogevoeligheid van het type cliënt, zakelijke relatie, product of transactie.[22]

Voor de risicoanalyse op het niveau van de instelling gelden de volgende opmerkingen:

- Hoewel de supranationale en nationale risicoanalyse een ander bereik hebben dan de individuele risicoanalyse van de instelling, neemt de instelling ook deze risicoanalyses in acht voor het vaststellen van effectieve gedragslijnen, procedures en maatregelen.[23]
- De risico's die verbonden zijn aan cliënten, zakelijke relaties, producten of transacties beïnvloeden het risicoprofiel van de instelling en bepalen mede de risico's waaraan de instelling is blootgesteld.

16 Zie: https://www.dnb.nl/media/2vqbu1cv/good-practices-integriteitrisicoanalyse.pdf. Dit document zal op voorzienbare termijn worden herzien.
17 Art. 2b lid 2 Wwft.
18 Zie: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554.
19 NRA Witwassen, NRA Terrorismefinanciering.
20 Art. 2b lid 1 Wwft.
21 Art. 2b lid 2 Wwft.
22 Art. 3 lid 8, 9 Wwft.
23 Art. 2c lid 1 Wwft. *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 43.

**QA.2.4: Vraag**
Hoe vaak moet een risicoanalyse worden bijgewerkt?

**Antwoord**
Er is geen specifieke termijn. Van een instelling wordt verwacht dat zij de identificatie en beoordeling van risico's actueel houdt door deze op gezette tijden en ook naar aanleiding van wijzigingen in bijvoorbeeld de dienstverlening of bedrijfsvoering te herhalen. De risicoanalyse dient de instelling in staat te stellen haar beleid vorm te geven, ten einde de geïdentificeerde risico's adequaat te beheersen.[24] Er is dus sprake van een cyclisch proces. Hoe vaak en op welke momenten de risicoanalyse wordt herzien is afhankelijk van de bedrijfsvoering (met factoren als omloopsnelheid cliënten, transacties, introductie van nieuwe producten) en de mate waarin externe ontwikkelingen plaatsvinden (zoals geopolitieke ontwikkelingen of wijzigingen in wetgeving). Ook incidenten of media aandacht kunnen aanleiding zijn om de risicoanalyse bij te werken

**QA.2.5: Vraag**
Wie is verantwoordelijk voor de risicoanalyse?

**Antwoord**
De risicoanalyse ziet op de risico's die de instelling loopt en ligt ten grondslag aan een goede beheersing. De instelling is verantwoordelijk voor de naleving van de Wwft. De risicoanalyse is een belangrijk sturingsinstrument voor het bestuur waar de verdere inrichting van de beheersmaatregelen van de instelling (zie 2.1.2) mede op is gebaseerd. Daarmee is de risicoanalyse ook van belang voor de andere functies binnen de instelling.

**QA.2.6: Vraag**
Hoe diepgaand moeten risico's geanalyseerd worden?

**Antwoord**
De risicoanalyse voorziet in een analyse van de integriteitsrisico's waar een specifieke instelling mee te maken krijgt in haar bedrijfsvoering. De risico's met betrekking tot witwassen en financieren van terrorisme die zich bij de instelling voordoen en de wijze waarop ze zich kunnen voordoen, zijn in beeld gebracht. De risicobeoordeling wordt afgestemd op de aard en omvang van de instelling.[25]
De risicoanalyse stelt de instelling in staat om passende beheersmaatregelen te nemen.[26] Meer waar het moet, minder waar het kan.

### GP2.1: Good practice – onderhouden van de risicoanalyse
Een instelling heeft een proces ingericht om te borgen dat *lessons learned* van incidenten, maar bijvoorbeeld ook FIU meldingen en thematische analyses, meegenomen worden in de periodieke update van de risicoanalyse. Ingrijpende incidenten leiden direct tot een herijking van de risicoanalyse. Iedere functie draagt vanuit de eigen rol bij aan een goede risicoanalyse.
Dit wordt in het proces van totstandkoming en actualisering vastgelegd.

### GP2.2: Good practice – analyse van de cliëntportfolio
Een instelling voert een diepgaande analyse van de cliëntportfolio uit om vast te stellen wat haar blootstelling is op klantgroepen of sectoren die inherent een hoger risico meebrengen op witwassen en/of het financieren van terrorisme. De uitkomsten van deze analyse zijn input voor de risicoanalyse.

Voor meer voorbeelden wordt verwezen naar de Good Practice SIRA.[27]

24 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 43.
25 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 42.
26 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 43.
27 Link: https://www.dnb.nl/media/2vqbuncv/good-practices-integriteitrisicoanalyse.pdf. Dit document zal op voorzienbare termijn worden herzien.

### 2.1.2 Beheersmaatregelen

De risicoanalyse verschaft inzicht in de risico's op witwassen en terrorismefinanciering waaraan een instelling is blootgesteld als gevolg van haar bedrijfsvoering. Om deze risico's te beperken en effectief te beheersen, beschikt een instelling over gedragslijnen, procedures en maatregelen.[28]
Dit geheel wordt in deze Q&A's/Good Practices ook wel aangeduid met 'beheersmaatregelen'.

Ze worden goedgekeurd door de personen die het dagelijks beleid van een instelling bepalen.[29]

### Q&A

**QA.2.7: Vraag**
Schrijft de Wwft voor iedere instelling dezelfde beheersmaatregelen voor?

**Antwoord**
Nee. De beheersmaatregelen die de instelling vaststelt, zijn evenredig aan de aard en de omvang van de instelling.[30] De beheersmaatregelen behoren dus te passen bij de omvang en aard van de instelling, en gericht te zijn op het effectief beperken en beheersen van de risico's op witwassen en financieren van terrorisme. Dat betekent dat een instelling met hoge risico's in principe over meer uitgebreide beheersmaatregelen beschikt dan een instelling met relatief lage risico's. De beheersmaatregelen zijn daarmee instellingspecifiek. Aan de door de instelling genomen beheersmaatregelen dient een risicoanalyse ten grondslag te liggen

**QA.2.8: Vraag**
Zijn er elementen waarop de beheersmaatregelen altijd moeten zien?

**Antwoord**
De beheersmaatregelen moeten ervoor zorgen dat instellingen de risico's op witwassen en financieren van terrorisme beperken en effectief beheersen.[31] Zij moeten, naast de risico's op witwassen en terrorismefinanciering waaraan een instelling zelf is blootgesteld, ook de voor de instelling relevante risico's die zijn geïdentificeerd in de supranationale risicobeoordeling en de nationale risicobeoordeling, adresseren.[32]

De beheersmaatregelen moeten in ieder geval invulling geven aan de verplichtingen ten aanzien van:
- risicomanagement (art. 1f t/m 2d Wwft)
- groepen (art. 2e en 2f Wwft)
- cliëntenonderzoek (art. 3 t/m 11 Wwft)
- melden van ongebruikelijke transacties (art. 16 t/m 20 Wwft)
- bewaren van bewijsstukken (art. 33 t/m 34a Wwft)
- doorlichten en opleiden van medewerkers (art. 35 Wwft). [33]

28 Art. 2c lid 1 Wwft.
29 Art. 2c lid 3 Wwft.
30 Art. 2c lid 2 Wwft.
31 Art. 2c lid 1 Wwft.
32 Art. 2c lid 1 Wwft; *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 43.
33 Art. 2c lid 2 Wwft.

**QA.2.9: Vraag**
Waarom moeten medewerkers opgeleid worden?

**Antwoord**
Instellingen zorgen ervoor dat medewerkers, voor zover relevant voor de uitoefening van hun taken en rekening houdend met de risico's, aard en omvang van de instelling, bekend zijn met de bepalingen van de Wwft.[34] Daarbij moeten medewerkers in staat zijn om ongebruikelijke transacties te herkennen, en om te handelen indien men op een ongebruikelijke transactie stuit.[35]

Training en opleiding zijn belangrijk bij een risicogebaseerde benadering, aangezien het eigen oordeel van (de beleidsbepalers en medewerkers van) een instelling in deze benadering een belangrijke rol speelt.[36] Toereikende bewustwording, ervaring en kennis van beleidsbepalers en van medewerkers met betrekking tot de beheersing van de risico's van witwassen en terrorismefinanciering zijn belangrijke voorwaarden voor een effectief beheersingskader.

---

**QA.2.10: Vraag**
Moeten medewerkers worden gescreend?

**Antwoord**
Ja. Instellingen dragen er zorg voor dat medewerkers, voor zover relevant voor de uitoefening van hun taken en rekening houdend met de risico's, aard en omvang van de instelling, worden doorgelicht.[37]

De FATF geeft in haar aanbevelingen aan dat een instelling adequate 'screening procedures' dient te hebben om zich te verzekeren van hoge standaarden bij het aanstellen van (nieuwe) werknemers.

Deze procedures dienen afgestemd te zijn op de risico's, aard en omvang van de instelling en de taken van de werknemer.[38] De screeningsautoriteit Justis biedt op haar website handvatten voor het screenen van personeel.[39]

## GP2.3: Good practice – Opleiding & training

Omdat integriteitrisico's dynamisch zijn en de beheersing daaraan wordt aangepast, evalueert en herziet een instelling de inhoud van haar opleidingen regelmatig. Om op de hoogte te blijven van de nieuwe ontwikkelingen en de bewustwording blijvend te bevorderen, biedt de instelling de opleidingen regelmatig aan.

Het aanbod is toegespitst op de verschillende functies binnen de instelling.
- CDD-analisten leren het cliëntenonderzoek goed en volledig uit te voeren en zogenoemde 'red flags' tijdig te signaleren.
- De compliancefunctie volgt aanvullende opleidingen om op de hoogte te blijven van ontwikkelingen inzake witwas- en terrorismefinancieringsrisico's en inzake wet- en regelgeving.
- De dagelijks beleidsbepalers krijgen opleidingen om hun (eind)verantwoordelijkheid te kunnen dragen.
- Het personeel dat cliënten werft en producten verkoopt, wordt op de hoogte gebracht van de bepalingen uit de Wwft door middel van trainingen zodat zij die ook meenemen in de uitvoering van hun werkzaamheden.

34 Art. 35 Wwft.
35 *Kamerstukken II* 2007-2008, 31 238, nr. 3, p. 35.
36 *Kamerstukken II* 2007-2008, 31 238, nr. 3, p. 35.
37 Art. 35 Wwft.
38 FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012-2023, p. 85.
39 www.justis.nl/producten/verklaring-omtrent-het-gedrag-vog/documenten-vog.

Naast het aanbod van (verplichte) e-learnings en onsite trainingen, organiseert de instelling regelmatig kennissessies waar witwastechnieken, methodes en trends worden besproken, en waar medewerkers gerichte casussen kunnen inbrengen.

De instelling legt het aanbod, de gevolgde trainingen, de frequentie en wie opleidingen volgen vast. Dit stelt haar in staat om het kennisniveau binnen de organisatie doorlopend vast te stellen, te monitoren en daarop in te spelen.

### 2.1.3 Toetsen beheersmaatregelen en controleren naleving

Het is van belang dat een instelling niet alleen beschikt over beheersmaatregelen, maar deze ook uitvoert.[40] Daarnaast is het van belang dat de beheersmaatregelen effectief zijn, zodat deze de risico's beperken en beheersen.

In dit verband schrijft de Wwft voor dat een instelling zorgdraagt voor een systematische toetsing van de gedragslijnen, procedures en maatregelen.[41] Indien een instelling daarover beschikt controleert de compliancefunctie de naleving van wettelijke regels en interne regels die de instelling zelf heeft opgesteld.[42] Een eventueel ingestelde auditfunctie controleert naast de naleving van de bij of krachtens de Wwft gestelde regels ook de uitoefening van de compliancefunctie.[43]

#### Q&A

**QA.2.11: Vraag**

Wat is systematische toetsing?

**Antwoord**

Een instelling toetst met regelmaat ('systematisch') de beheersmaatregelen. Waar nodig worden deze aangepast, mede op basis van de actualisering van de risicobeoordeling van de instelling.[44]
Bij toetsing gaat de instelling dus na of de beheersmaatregelen effectief zijn, zodat deze de risico's beperken en beheersen. Daarbij gaat de instelling ook na of er sprake is van veranderingen in de risico's, waardoor aanpassing van de beheersmaatregelen nodig kan zijn. De instelling legt dit vast.

---

**QA.2.12: Vraag**

Welke controles en toetsingen voert de compliancefunctie uit?

**Antwoord**

Indien een instelling over een onafhankelijke compliancefunctie beschikt, controleert deze de naleving van de wettelijke regels en van de regels die een instelling zelf heeft opgesteld.[45] Dit houdt ook in dat erop wordt toegezien dat procedures, bijvoorbeeld voor het verrichten van cliëntenonderzoek, in overeenstemming zijn met geldende regelgeving.[46]

40 Art. 2c lid 4 en art. 2d lid 3, 4 Wwft. Vgl. ECLI:NL:RBROT:2015:5635.
41 Art. 2c lid 4 Wwft.
42 Art. 2d lid 3 Wwft.
43 Art. 2d lid 4 Wwft.
44 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 44.
45 Art. 2d lid 3 Wwft.
46 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 44.

Daarnaast heeft de compliancefunctie ook een rol bij de toetsing of de getroffen beheersmaatregelen effectief zijn.

**QA.2.13: Vraag**
Is elke instelling verplicht te voorzien in de invulling van een afzonderlijke compliancefunctie?

**Antwoord**
Dat hangt ervan af. Voor zover passend bij de aard en omvang van de instelling, beschikt een instelling over een onafhankelijke en effectieve compliancefunctie.[47]
Voor een instelling van beperkte omvang kan het onevenredig en daarmee niet passend zijn om een afzonderlijke compliancefunctie in te richten. De omvang van de instelling, alsmede het type instelling, speelt een belangrijke rol bij de naleving van deze verplichting.[48]

Verder kan de wijze waarop de compliancefunctie wordt ingericht op de aard en omvang van de instelling worden afgestemd. De compliancefunctie dient op onafhankelijke en effectieve wijze te worden uitgevoerd. In beginsel betekent dit dat de personen die betrokken zijn bij de uitoefening van de compliancefunctie, niet tevens betrokken zijn bij de activiteiten waarop zij toezicht houden. Echter, bij kleinere instellingen kan het onevenredig zijn om de onafhankelijkheid van de compliancefunctie op deze wijze vorm te geven. Uiteindelijk ziet het bestuur van de instelling toe op de naleving van de Wwft.
Een instelling kan ervoor kiezen om de compliancefunctie (geheel of gedeeltelijk) uit te besteden.[49]
De uitbesteding is passend bij de aard en omvang van de instelling.

**QA.2.14: Vraag**
Wat is de rol van de auditfunctie ten aanzien van de Wwft?

**Antwoord**
Indien van toepassing en voor zover passend bij de aard en de omvang van de instelling, draagt een instelling er zorg voor dat op onafhankelijke wijze een auditfunctie wordt uitgeoefend ten aanzien van haar werkzaamheden.[50] De auditfunctie controleert op onafhankelijke wijze de naleving van de Wwft door de instelling, alsmede de uitoefening van de compliancefunctie. Dat omvat ten minste het controleren van de werking van de beheersmaatregelen.
De intensiteit van de invulling van de auditfunctie zal afhangen van het risicoprofiel van de instelling. Voor de invulling die wordt gegeven aan de mate van onafhankelijkheid van de auditfunctie geldt dat dit afhankelijk is van de aard en omvang van de instelling.[51]
Ook de auditfunctie kan geheel of gedeeltelijk uit worden besteed.[52]

47 Art. 2d lid 2 Wwft.
48 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 44.
49 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 44. Trustkantoren mogen op grond van art. 16 lid 2 Wtt 2018 de compliancefunctie niet uitbesteden.
50 Art. 2d lid 4 Wwft.
51 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 45.
52 *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 44.

## GP2.4: Good practice – Compliancefunctie

Een instelling heeft de positie van de compliancefunctie vastgelegd in een zogenoemd compliance charter. Hierin is onder andere vastgelegd dat de compliance officer toegang heeft tot alle informatie, tot alle ruimtes en tot alle personen binnen de organisatie. Ook is vastgelegd aan wie de compliancefunctie rapporteert en dat de compliancefunctie rechtstreeks toegang heeft tot de raad van commissarissen. De instelling heeft bij het opstellen van het charter de EBA Guidelines over dit onderwerp betrokken.[53]

## GP2.5: Good practice – Auditfunctie

Bij het inrichten van de auditfunctie heeft een instelling in ieder geval rekening gehouden met de volgende punten:

- De auditfunctie opereert onafhankelijk.
- De auditfunctie controleert ten minste een keer per jaar de naleving van de Wwft en de uitoefening van de compliancefunctie.
- De auditfunctie legt de bevindingen vast in een rapport.
- Geconstateerde bevindingen worden door de instelling vertaald naar aanscherping van de maatregelen. De auditfunctie stelt vervolgens vast in hoeverre dit voldoende is.

## GP2.6: Good practice – Toetsing opleidingen

Een instelling heeft een Wwft-opleidingsprogramma voor haar medewerkers. De compliance-functie toetst jaarlijks of de opleidingen effectief zijn door na te gaan of medewerkers de voor hun functie relevante risico's kennen, of zij de risico's herkennen in concrete gevallen en of zij in die gevallen de passende maatregelen nemen. De compliancefunctie voert deze toets o.a. uit aan de hand van concrete cliëntendossiers en van uitgevoerde transacties.

### 2.1.4 Bijstellen

Uit de systematische toetsing en het controleren van de naleving kan blijken dat de beheersmaatregelen passend zijn, en de risico's met betrekking tot witwassen en financieren van terrorisme effectief beperken en beheersen.

De uitkomst van de toetsing en de controle kan ook zijn dat:

- de beheersmaatregelen de risico's met betrekking tot witwassen en financieren van terrorisme onvoldoende beperken en beheersen
- de beheersmaatregelen onvoldoende worden nageleefd.

In deze laatste gevallen stelt de instelling de beheersmaatregelen bij, zodat deze passend zijn bij de risico's, of borgt de instelling de naleving.[54]

53 www.eba.europa.eu/eba-publishes-guidelines-role-and-responsibilities-amlcft-compliance-officer.
54 Art. 2c lid 4 Wwft. *Kamerstukken II* 2017-2018, 34 808, nr. 3, p. 44-45.

### G P2.7: Good practice – Bijstellen

De compliancefunctie van een instelling heeft vastgesteld dat beleid, procedures en maatregelen binnen een afdeling onvoldoende worden nageleefd. Hierdoor loopt de instelling ongewenste risico's met betrekking tot witwassen. De compliancefunctie bespreekt dit met het management van de afdeling. Dit leidt tot een rapportage aan het management van de afdeling, waarin ook de afgesproken acties zijn opgenomen. De Wwft-verantwoordelijke bestuurder en de auditfunctie ontvangen deze rapportage ook.

In overleg met het management wordt er een bijeenkomst belegd waarin de compliancefunctie de bevindingen terugkoppelt aan de medewerkers en waarin het management het belang van de afgesproken acties onderstreept. De compliancefunctie monitort de opvolging van de afgesproken acties, en rapporteert hierover aan het management van de afdeling en neemt dit ook op in de reguliere monitoringrapportage aan de Wwft-verantwoordelijke bestuurder.

## 2.2 Uitbesteding

Onder voorwaarden kunnen instellingen delen van het cliëntenonderzoek uitbesteden. De instelling die iets uitbesteedt, blijft in alle gevallen zelf volledig verantwoordelijk voor het naleven van de eisen van het cliëntenonderzoek. Onderdeel van die verantwoordelijkheid is dat de uitbestedende instelling ook altijd een effectieve controle heeft ingericht om te waarborgen dat het cliëntenonderzoek goed wordt uitgevoerd wanneer onderdelen van de uitvoering aan een ander zijn uitbesteed.
Het uiteindelijke besluit over het al dan niet accepteren van een cliënt en de hoogte van diens risicoprofiel wordt altijd (aantoonbaar) bij de instelling gelegd.

### Q&A

**QA.2.15: Vraag**
Welke onderdelen van het cliëntenonderzoek mag de instelling uitbesteden aan een derde?

**Antwoord**
Op grond van art. 10 Wwft is het instellingen toegestaan om onderdelen van het cliëntenonderzoek uit te besteden aan een ander, uit hoofde van een uitbesteding- of agentuurovereenkomst.

Een instelling kan het cliëntenonderzoek van art. 3 lid 2 Wwft op de volgende subonderdelen uitbesteden:

a. cliëntidentificatie en verificatie
b. UBO identificatie en verificatie
c. vaststellen doel en beoogde aard van de zakelijke relatie
d. verificatie bevoegdheid en identiteit van de vertegenwoordiger van een client
e. onderzoek of een client voor zichzelf optreedt, dan wel ten behoeve van een derde.

Van belang hierbij is dat de verantwoordelijkheid bij de uitbestedende instelling blijft liggen; alles wat de partij waaraan de diensten zijn uitbesteed doet, doet deze namens de uitbestedende instelling. Fouten en nalatigheden in het uitgevoerde cliëntenonderzoek komen dus voor rekening en risico van de uitbestedende instelling. De instelling blijft ook verantwoordelijk voor het actueel houden van de cliëntgegevens.

**QA.2.16: Vraag**
Wat is het verschil tussen uitbesteden en introduceren?

**Antwoord**
Als een instelling al cliëntonderzoek heeft verricht naar een cliënt en vervolgens deze cliënt introduceert bij een andere instelling, dan regelt art. 5 lid 1 Wwft onder welke voorwaarden de accepterende instelling op het cliëntenonderzoek van de introducerende instelling mag vertrouwen. Dat is een andere situatie dan het uitbesteden van het cliëntenonderzoek conform art. 10 Wwft. In die laatste situatie besteedt de instelling (een deel van) het bedrijfsproces uit aan een derde partij, die dat proces namens de instelling uitvoert. Bij de introductie van een cliënt op basis van art. 5 Wwft kan een instelling gebruikmaken van het onderzoek dat is uitgevoerd door een instelling die ook zelfstandig een verplichting heeft onder de Wwft om cliëntenonderzoek uit te voeren.

---

**QA.2.17: Vraag**
Voor welke onderdelen van het cliëntenonderzoek is uitbesteding niet toegestaan?

**Antwoord**
De instelling mag de voortdurende controle op de zakelijke relatie en transacties niet uitbesteden. De instelling dient zelf de zakelijke relatie te monitoren.

---

**QA.2.18: Vraag**
Aan welke eisen moet het uitbesteden van het cliëntonderzoek voldoen?

**Antwoord**
Als de instelling overgaat tot het uitbesteden van het cliëntenonderzoek aan een derde partij maakt de instelling een zichtbare risicoafweging. Deze ziet onder meer op de deskundigheid van deze derde partij en op hoe deze derde partij in de praktijk de Wwft voor de uitbestedende partij uitvoert.

Verder is het van belang dat de instelling niet alleen vastlegt dat de derde partij die (delen van) het cliëntenonderzoek voor de instelling uitvoert, voldoet aan de Wwft en waar nodig aan het beleid van de instelling, maar ook dat de instelling dit periodiek controleert en vaststelt.

**QA.2.19: Vraag**
Worden aan Nederlandse vergunninghoudende instellingen nog andere eisen gesteld aan uitbesteding?

**Antwoord**
Ja. Voor Nederlandse instellingen waaraan DNB een vergunning heeft verleend in het kader van de Wet op het financieel toezicht (Wft) gelden aanvullende eisen die ook relevant zijn bij het uitbesteden van onderdelen van het cliëntonderzoek aan een derde. Zo verlangt art. 3:17 Wft dat de bedrijfsvoering zodanig is inricht dat deze een beheerste en integere uitoefening van het bedrijf waarborgt. Art. 3:18 Wft geeft regels voor uitbesteding. De eisen die op grond hiervan aan uitbesteding worden gesteld, zijn nader uitgewerkt in Hoofdstuk 5 van het Besluit prudentiële regels Wft (Bpr).

## GP2.8: Good practice – Uitbestedingsbeleid

Een instelling heeft de gevolgen van mogelijke uitbestedingen goed in kaart gebracht in de vorm van algemeen uitbestedingsbeleid dat alle aspecten van uitbesteding omvat. De instelling heroverweegt regelmatig haar uitbestedingsbeleid en of zij met de uitbesteding het risico loopt dat naleving op de Wwft onvoldoende is gewaarborgd.

Bij het selecteren van de dienstverlener heeft de instelling vooraf een inschatting gemaakt dat de dienstverlener zorgvuldig uitvoering zal geven aan de uit te besteden werkzaamheden.
De instelling heeft dit schriftelijk vastgelegd in een due diligence beoordeling.

Het besluit tot het uitbesteden van Wwft-werkzaamheden wordt genomen door de directie. De dagelijkse beleidsbepaler die toezicht houdt op het naleven van de Wwft is ook betrokken geweest bij het nemen van besluiten over het uitbesteden van onderdelen van het cliëntenonderzoek aan de beoogde dienstverlener.

De instelling heeft gekozen om bepaalde delen van het cliëntenonderzoek uit te besteden aan een dienstverlener buiten de Europese Economische Ruimte. Gelet op de risico's die hiermee gepaard kunnen gaan heeft de instelling bijzondere aandacht besteed aan belangrijke punten. Zoals de bescherming van vertrouwelijke (persoons)gegevens en het waarborgen dat zij effectief toezicht kan houden op de partij waaraan de diensten zijn uitbesteed.

## GP2.9: Good practice – Uitbestedingsovereenkomst

In de uitbestedingsovereenkomst is de duur en de wijze van uitvoering van de uitbestede activiteiten per onderdeel beschreven. In de uitbestedingsovereenkomst is expliciet geregeld dat toezichthouders het recht hebben om onderzoek te verrichten en waar nodig rechtstreeks toegang krijgen tot relevante gegevens en vestigingen van de derde waaraan diensten zijn uitbesteed.

In het uitbestedingsbeleid en de uitbestedingsovereenkomst heeft de instelling bovendien geregeld of de partij aan wie is uitbesteed, zelf ook mag uitbesteden. Indien de uitbestedingsovereenkomst hier ruimte toe laat is wel opgenomen aan welke eisen dergelijke 'onder-uitbesteding' dient te voldoen. Dit zijn in ieder geval dezelfde regels als waaraan de oorspronkelijke partij waaraan is uitbesteed dient te voldoen, zoals het instructierecht van de uitbesteder en het recht op direct onderzoek en directe toegang.

## GP2.10: Good practice – Beoordeling uitvoering uitbesteding

Bij het gebruikmaken van een externe dienstverlener heeft een instelling goede afspraken gemaakt met de partij waaraan werkzaamheden zijn uitbesteed.

De instelling heeft voldoende kerncompetenties binnen de eigen organisatie in stand gehouden (in de vorm van deskundige compliance officers en auditors) om de uitvoering van de uitbesteding van CDD-operaties te kunnen beoordelen. De instelling kan aantonen dat zij de dienstverlener adequaat aanstuurt en controleert, en in het uiterste geval de rechtstreekse leiding over de uitbestede activiteit kan overnemen of voor de overdracht aan een andere geschikte partij kan zorgdragen.

Ook voert de instelling systematische controles uit op de uitbesteding om te bepalen of de uitbesteding in de praktijk werkt zoals vooraf beoogd en voldoet aan de wettelijke eisen. Processen, systemen en lijsten worden periodiek getest.

## GP2.11: Good practice – Delen vertrouwelijke gegevens

Een instelling die vertrouwelijke gegevens deelt in het kader van een uitbesteding, kan aantonen dat zij van de dienstverlener met wie zij deze gegevens deelt vereist dat deze de vertrouwelijkheid en informatiebeveiliging op minimaal hetzelfde niveau waarborgt als de instelling zelf.

Hierbij hanteert de instelling het uitgangspunt dat geen informatie met deze partij wordt gedeeld anders dan noodzakelijk voor de uitvoering van de uitbestede werkzaamheden.

Zie voor meer *good practices* de DNB guidance: Good practices beheersing risico's bij uitbesteding (dnb.nl).

## 2.3 Interne Klokkenluiderregeling en meldpunt misstanden

Het is belangrijk dat misstanden in de financiële sector gemeld en onderzocht kunnen worden. Dit draagt bij aan een integere financiële sector en aan financiële stabiliteit. Daarom moeten instellingen volgens de Wwft en de Wet bescherming klokkenluiders een interne meldprocedure inrichten voor het omgaan met het melden van vermoedelijke misstanden binnen hun organisatie.[55]

DNB beschikt als bevoegde autoriteit ook over een procedure voor meldingen van mogelijke of werkelijke misstanden bij onder toezicht staande instellingen.[56]

### Q&A

**QA.2.20: Vraag**
Bij welke omvang moet een instelling een interne meldprocedure inrichten voor het omgaan met het melden van misstanden binnen de organisatie?

**Antwoord**
Ja. De Wwft vereist dat een instelling beschikt over adequate voorzieningen, die passend zijn bij de aard en omvang van de instelling en die het haar medewerkers mogelijk maken om een overtreding van de Wwft intern en op anonieme wijze te melden via een specifiek, onafhankelijk kanaal.[57] Instellingen moeten daarnaast altijd, ongeacht het aantal personen dat bij hen werkzaam zijn, voldoen aan de vereisten van die de Wet bescherming klokkenluiders stelt aan een interne meldprocedure. Voor instellingen geldt namelijk niet de regel dat deze vereisten alleen van toepassing zijn als zij ten minste 50 personen in dienst hebben.[58]

**QA.2.21: Vraag**
Wie kan een overtreding van de Wwft of een misstand melden?

**Antwoord**
Iedere natuurlijke persoon die in de context van diens werkgerelateerde activiteiten een vermoeden van een misstand heeft, kan dit melden – de melder valt in dit geval onder de definitie van een klokkenluider.

---

**QA.2.22: Vraag**
Heeft DNB een meldpunt?

**Antwoord**
Ja. Personen die een vermoeden hebben van een misstand – waaronder een overtreding van de Wwft – bij een onder het toezicht van DNB staande instelling, kunnen een melding doen bij het DNB Meldpunt Misstanden. Meer informatie hierover en over het doen van een melding is te vinden op de website van DNB.[59]

55 Art. 20a lid 1 Wwft.
56 Art. 20a lid 2 Wwft.
57 Art. 20a lid 1 Wwft.
58 Art. 2 lid 3 Wet bescherming klokkenluiders.
59 Voor meer informatie: www.dnb.nl/contact/bezwaar-klacht-of-misstand-melden/melden-misstanden-financiele-instellingen/.

**QA.2.23: Vraag**
Moet ik eerst een melding doen bij mijn eigen organisatie voordat ik een melding kan doen bij DNB?

**Antwoord**
Nee, een klokkenluider mag bij een vermoeden van een misstand direct een melding doen bij DNB. Waar passend, heeft het de voorkeur dat een misstand eerst intern bij de instelling wordt gemeld, bijvoorbeeld door gebruik te maken van een interne klokkenluidersregeling.

---

**QA.2.24: Vraag**
Wat is de rol van het Huis voor klokkenluiders?

**Antwoord**
Het Huis voor klokkenluiders heeft verschillende taken, onder andere het geven van advies aan werknemers die bij maatschappelijke misstanden als 'klokkenluider' aan de bel trekken, onderzoek naar misstanden en onderzoek naar de behandeling van een klokkenluider.
Meer informatie hierover is te vinden op de website van het Huis voor klokkenluiders.[60]

## 2.4 WTR2

Het betalingsverkeer kan misbruikt worden voor het financieren van terrorisme en het witwassen van geld. De WTR2 bevat bepalingen om informatie vast te leggen over geldovermakingen en heeft als doel om inzicht te krijgen in de herkomst en bestemming van gelden.[61]

Aangewezen instellingen zijn verplicht om specifieke informatie aan elkaar door te geven over de verzender en de begunstigde in de keten van geldovermakingen. Deze informatie is van groot belang om terrorismefinanciering en witwassen te kunnen detecteren.

### Q&A

**QA.2.25: Vraag**
Op welke geldovermakingen is de WTR2 van toepassing?

**Antwoord**
De WTR2 is van toepassing op geldovermakingen verzonden of ontvangen door betalingsdienst-aanbieders in de Europese Unie, of waar zij als intermediair optreden.[62] De WTR2 is niet van toepassing wanneer geldovermakingen worden verricht met krediet- of debetkaarten, elektronischgeld-instrumenten, of met mobiele telefoons of vergelijkbare apparaten. Dit middel moet dan wel uitsluitend worden gebruikt voor de betaling van goederen of diensten. Het is wel verplicht dat het nummer van het middel wordt gevoegd bij alle overmakingen die uit de betreffende transactie voortvloeien.

60 www.huisvoorklokkenluiders.nl.
61 Verordening (EU) 2015/847 van het Europees Parlement en de Raad van 20 mei 2015 betreffende bij geldovermakingen te voegen informatie en tot intrekking van Verordening (EG) nr. 1781/2006, PbEU 2015, L141/1, zoals nadien gewijzigd.
62 Art. 2 WTR2.

**QA.2.26: Vraag**
Op welk onderdeel van de geldovermakingen is de WTR2 van toepassing?

**Antwoord**
De kern van de WTR2-verplichtingen betreft het registreren van specifieke informatie van de verzender én de begunstigde door de gehele keten. Hierbij moeten de herkomst en bestemming van gelden inzichtelijk worden gemaakt.

**QA.2.27: Vraag**
Wat is bij een geldovermaking de verantwoordelijkheid van enerzijds de betaaldienstaanbieder van de betaler en anderzijds de betaaldienstaanbieder van de begunstigde?

**Antwoord**
De WTR2 bepaalt welke informatie bij de geldovermaking moet worden vastgelegd en bijgevoegd: De betaaldienstaanbieder van de betaler draagt zorg voor een adequate informatievastlegging.[63] De betaaldienstaanbieder van de begunstigde en eventuele intermediaire betaaldienstverleners controleren of de informatie die zij bij de betaling ontvangen, compleet is.[64]

Indien geconstateerd wordt dat informatie onvolledig is, dient de instelling een risicogebaseerde afweging te maken of de geldovermaking geweigerd, opgeschort of uitgevoerd kan worden – waarbij de ontbrekende informatie dient te worden opgevraagd.[65]

De Gemeenschappelijke Richtsnoeren (Joint Guidelines) van de Europese Toezichthoudende autoriteiten (EBA, EIOPA en ESMA) bevatten een nadere toelichting.[66]

**QA.2.28: Vraag**
In hoeverre is de WTR2 van toepassing op geldovermakingen buiten de EU?

**Antwoord**
De WTR2 is van toepassing op geldovermakingen binnen de EU, ongeacht de valuta.[67]

**QA.2.29: Vraag**
Hoe gaat een betaaldienstaanbieder om met ontbrekende informatie over de betaler of de begunstigde?

**Antwoord**
In de Gemeenschappelijke Richtsnoeren (Joint Guidelines) van de Europese Toezichthoudende autoriteiten (EBA, EIOPA en ESMA) over WTR2 wordt omschreven hoe instellingen om kunnen gaan met ontbrekende informatie van een geldovermaking en welke procedures zij dienen in te voeren voor het omgaan met geldovermakingen waarbij informatie ontbreekt.

63 Art. 4 WTR2.
64 Art. 7 WTR2 en art 11 WTR2.
65 Artt. 8, 12 WTR2.
66 EBA, ESMA & EIOPA, Gemeenschappelijke richtsnoeren uit hoofde van artikel 25 van Verordening (EU) 2015/847 over de maatregelen die betalingsdienstaanbieders dienen te nemen om ontbrekende of onvolledige informatie over de betaler of de begunstigde op te sporen, en de procedures die zij dienen in te voeren voor het omgaan met geldovermakingen waarbij de vereiste informatie ontbreekt, 2017.
67 Art. 2 lid 1 WTR2.

**QA.2.30: Vraag**
Wat is de relatie tussen de WTR2 en de aanstaande Transfer of Funds Regulation (TFR)?

**Antwoord**
De WTR2 wordt vervangen door de TFR.[68] De TFR is vanaf 30 december 2024 van toepassing.
Er zijn twee belangrijke verschillen tussen de WTR2 en de TFR:

- De TFR breidt de toepassing uit naar cryptodienstverleners die vallen onder de reikwijdte van de Markets in Crypto Assets Regulation MiCAR.[69]
- Bij cryptotransacties geldt de verplichting om informatie bij transacties te voegen ongeacht de omvang van de transactie. Bij transacties door betaaldienstverleners en kredietinstellingen laat de Verordening ruimte aan de lidstaten om een drempel van € 1.000 te hanteren.

## 2.5 Bescherming persoonsgegevens

De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht.[70] Persoonsgegevens, die zijn verzameld op grond van de Wwft, worden door een instelling verwerkt met het oog op het voorkomen van witwassen en financieren van terrorisme en worden niet verder verwerkt voor commerciële doeleinden of andere doeleinden die niet verenigbaar zijn met dat doel.[71]

### Q&A

**QA.2.31: Vraag**
Rechtvaardigt de wettelijke grondslag in de Wwft elke vorm van gegevensverwerking door instellingen als dat het doel van het voorkomen van witwassen en financieren van terrorisme dient?

**Antwoord**
Nee, het hebben van een wettelijke grondslag rechtvaardigt niet elke vorm van gegevenswerking. Het is van belang dat financiële instellingen de overige vereisten en beginselen van de Algemene Verordening Gegevenswerking (AVG) in acht (blijven) nemen.[72] De gegevensverwerking behoort noodzakelijk te zijn en de belangen van de betrokkenen behoren afgewogen te worden tegen het belang van de verwerkingsverantwoordelijke.

Belangrijke principes zijn *proportionaliteit* en *subsidiariteit*. De inbreuk op het recht op privacy moet in verhouding staan tot het doel (proportionaliteit). Daarnaast moet er geen andere manier zijn waarop het doel bereikt kan worden waarvoor de gegevens worden verwerkt die minder nadelig is voor de betrokkenen (subsidiariteit). De gegevensverwerking is onrechtmatig als niet wordt voldaan aan deze beginselen en andere vereisten uit de AVG.

68 Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende bij geldovermakingen van geld en van bepaalde cryptoactiva te voegen informatie en tot intrekking van Verordening (EG) nr. 1781/2006.
69 Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactivamarkten en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937.
70 Art. 10 Grondwet; Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), overweging 1.
71 Art. 34a lid 1 Wwft.
72 Zie ook Grondslagen AVG uitgelegd | Autoriteit Persoonsgegevens

**QA.2.32: Vraag**

Worden cliënten ook op de hoogte gesteld dat persoonsgegevens worden verwerkt?

**Antwoord**

Ja. Een instelling informeert de cliënt over de verplichtingen uit de Wwft en de daarmee samenhangende verwerking van persoonsgegevens.[73] Dit omvat onder meer het informeren van cliënten over het doel van de verwerking van de gegevens en de wettelijke bewaartermijn die geldt ten aanzien van deze gegevens. Een belangrijke kanttekening is dat een instelling de client niet mag informeren over meldingen gedaan aan de FIU-NL (zie QA4.25).

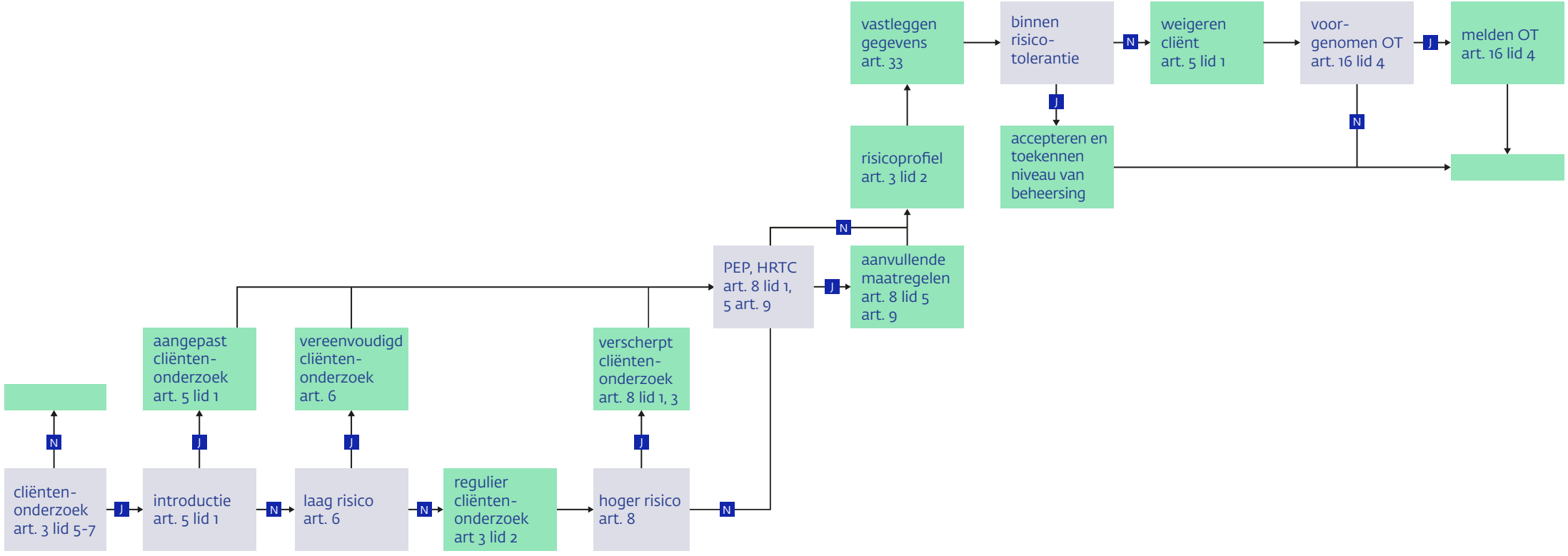
73 Art. 34a lid 2 Wwft, art. 5.1a AVG.

# 3 Cliëntenonderzoek: cliëntacceptatie

Dit hoofdstuk gaat in op het cliëntenonderzoek en op de cliëntacceptatie als mogelijke uitkomst daarvan. Cliëntenonderzoek is verplicht op grond van art. 3 Wwft. Het stelt de instelling onder andere in staat om de cliënt en de UBO's te identificeren en de identiteit daarvan te verifiëren, het doel en de beoogde aard van de zakelijke relatie vast te stellen, en een voortdurende controle uit te oefenen. In het verlengde daarvan ligt dat het de instelling in staat stelt het risico te beoordelen, op basis waarvan de instelling bepaalt of een standaard onderzoek of eventueel een vereenvoudigd of juist verscherpt cliëntenonderzoek dient plaats te vinden.

Instellingen mogen het cliëntenonderzoek in belangrijke mate risicogebaseerd invullen. Dit betekent echter niet dat het achterwege mag worden gelaten. Het cliëntenonderzoek moet kortom altijd worden uitgevoerd. Uiteindelijk stelt de instelling met hulp van de informatie uit het cliënten-onderzoek een risicoprofiel op van de cliënt. Hierbij legt de instelling de verzamelde gegevens vast, en beoordeelt de instelling of de cliënt past binnen haar risicotolerantie en of de cliënt kan worden geaccepteerd of geweigerd.

Het bijbehorende stroomschema kan worden beschouwd als een hulpmiddel bij het lezen van dit hoofdstuk en als een manier om de verschillende onderdelen van het cliëntenonderzoek in kaart te brengen.


cliënten-onderzoek art. 3 lid 5-7
N
aangepast cliënten-onderzoek art. 5 lid 1
J
introductie art. 5 lid 1
N
vereenvoudigd cliënten-onderzoek art. 6
J
laag risico art. 6
N
regulier cliënten-onderzoek art 3 lid 2
verscherpt cliënten-onderzoek art. 8 lid 1, 3
J
hoger risico art. 8
N
PEP, HRTC art. 8 lid 1, 5 art. 9
J
aanvullende maatregelen art. 8 lid 5 art. 9
N
risicoprofiel art. 3 lid 2
vastleggen gegevens art. 33
binnen risico-tolerantie
N
weigeren cliënt art. 5 lid 1
J
accepteren en toekennen niveau van beheersing
voor-genomen OT art. 16 lid 4
J
melden OT art. 16 lid 4
N

## 3.1 Zakelijke relatie of relevante incidentele transactie

Met het cliëntenonderzoek komen instellingen te weten met wie zij zaken doen. Het onderzoek is afhankelijk van de cliënt en de risico's die de instelling ziet en wordt hier aantoonbaar op afgestemd.[74] In onder meer de volgende gevallen moet cliëntenonderzoek worden verricht:[75]

- Bij het aangaan van een zakelijke relatie. Dat is een zakelijke, professionele, of commerciële relatie tussen een instelling en een natuurlijke persoon, rechtspersoon of vennootschap, die verband houdt met de professionele activiteiten van die instelling en waarvan op het tijdstip dat het contact wordt gelegd, wordt aangenomen dat deze enige tijd zal duren.[76]
- Waar er geen sprake is van een zakelijke relatie: bij een incidentele transactie verricht ten behoeve van de cliënt van ten minste EUR 15.000, of twee of meer transacties waartussen een verband bestaat met een gezamenlijke waarde van ten minste EUR 15.000.[77]

In beginsel vindt het cliëntenonderzoek plaats vóórdat de instelling een zakelijke relatie aangaat of een incidentele transactie uitvoert.[78]

### GP3.1: Good practice – aantoonbaar afstemmen van cliëntenonderzoek in de praktijk

- Een instelling heeft intern beleid opgesteld hoe de risicobeoordeling van een cliënt wordt gedaan. De risicobeoordeling wordt conform dit beleid uitgevoerd en vastgelegd in het dossier van de cliënt. Hierbij houdt de instelling rekening met de risico's die het type cliënt, de zakelijke relatie, het product of de transactie meebrengen.
- De compliancefunctie controleert vervolgens of het cliëntenonderzoek aantoonbaar is afgestemd op de risicogevoeligheid voor witwassen of financieren van terrorisme van het type cliënt, de zakelijke relatie, het product of de transactie.

## 3.2 Geïntroduceerde cliënt

Een instelling hoeft niet zelf het cliëntenonderzoek te verrichten, maar kan ook afgaan op het cliëntenonderzoek dat is gedaan door een andere Wwft-plichtige instelling (de introducerende partij).[79] Zowel de accepterende instelling als de introducerende instelling hebben allebei een eigen verantwoordelijkheid voor naleving van de op hen rustende verplichtingen ten aanzien van het cliëntenonderzoek. Dit geldt ook voor de vastlegging van dit onderzoek.

Introductie kan plaatsvinden in de volgende situaties:[80]

- Een instelling verricht diensten voor een cliënt die al cliënt is bij een andere instelling, of Een instelling brengt een eigen cliënt aan bij een andere instelling.

74 Art. 3 lid 8 Wwft.
75 Art. 3 lid 5 Wwft. Zie dit artikel voor het gehele overzicht van gevallen waarin cliëntenonderzoek moet worden verricht.
76 Art. 1 lid 1 Wwft.
77 Uit de wetsgeschiedenis kan worden opgemaakt dat bij elke individuele money transfer (d.i. een geldtransfer in de zin van richtlijn (EU) 2015/2366) een zakelijke relatie moet worden verondersteld. Zie: Kamerstukken II 2007-2008, 31 238, nr. 3, p. 12; Kamerstukken II 2011-2012, 33 238, nr. 3, p. 4.
78 Art. 4 lid 1 en art. 5 lid 1 Wwft. De uitzonderingen hierop staan in artikel 4 Wwft (zie bijvoorbeeld artikel 4 lid 3 Wwft).
79 Art. 5 lid 1 onder a Wwft specificeert welke instellingen cliënten kunnen introduceren. Indien er sprake is van een andere derde partij kan geen gebruik worden gemaakt van artikel 5 Wwft. Mogelijk kan wel gebruik worden gemaakt van uitbesteding zoals beschreven in art. 10 Wwft.
80 Kamerstukken II 2007-2008, 31 238, nr. 3, p. 23.

## Q&A

**QA3.1: Vraag**
Is het voor de accepterende instelling voldoende om een bevestiging te hebben van de introducerende instelling?

**Antwoord**
Nee, een accepterende instelling moet bij introductie beschikken over de gegevens die zijn gebruikt bij het cliëntenonderzoek door de introducerende instelling.[81] Daarnaast moet de accepterende instelling beschikken over de onderliggende documentatie waarop de acceptatie van de cliënt is gebaseerd.

---

**QA3.2: Vraag**
Kan bij introductie het risicoprofiel van de cliënt worden overgenomen van de introducerende instelling?

**Antwoord**
Nee, de accepterende instelling is zelf verantwoordelijk voor het opstellen van het risicoprofiel en moet daarvoor beschikken over de juiste gegevens.

---

**QA3.3: Vraag**
Wat als de introducerende partij de gegevens van de cliënt niet kan verstrekken?

**Antwoord**
Indien de introducerende instelling de gegevens niet kan verstrekken, verricht de accepterende instelling alsnog het cliëntenonderzoek dat op grond van de Wwft noodzakelijk is.

**QA3.4: Vraag**
Moet de eigen cliënt op het moment dat hij wordt geïntroduceerd bij een andere instelling toestemming geven voor het verstrekken van zijn persoonsgegevens aan deze andere instelling?

**Antwoord**
Ja, in lijn met art. 6 Algemene Verordening Gegevensverwerking (AVG) dient toestemming gevraagd te worden aan de cliënt. Hoewel de zogenoemde 'doelbinding' in feite is geregeld in art. 34a Wwft, gaat de informatie nu naar een andere verwerker.

### GP3.2: Good practice – Controle tussenpersoon

In het beleid ten aanzien van identificatie en verificatie van cliënten legt een levensverzekeraar vast op welke manier wordt omgegaan met het vertrouwen op de door tussenpersonen uitgevoerde identificatie en verificatie. Ook ligt vast op grond waarvan, hoe en wanneer de betreffende tussenpersonen de gegevens omtrent de identificatie en verificatie van cliënten beschikbaar stellen.

81 Art. 33 lid 1 Wwft.

### GP3.3: Good practice – Controle procedures en maatregelen introducerende instelling

Een instelling gaat op risicogebaseerde wijze na of de introducerende instellingen adequate maatregelen hebben om uitvoering te geven aan het cliëntenonderzoek. Zo vraagt de instelling bij instellingen die per jaar gemiddeld meer dan 50 cliënten introduceren jaarlijks de Wwft-procedures op ter beoordeling. Bij instellingen die per jaar gemiddeld meer dan 100 cliënten introduceren wordt daarbij ook een accountantsverklaring opgevraagd over de werking van de Wwft-procedures. Bij andere instellingen gaat de instelling steekproefsgewijs de werking van het cliëntenonderzoek na.

## 3.3 Vereenvoudigd cliëntenonderzoek

De Wwft kent een risicogebaseerde benadering. Op basis van deze benadering kan uit een risicobeoordeling ook volgen dat een instelling kan volstaan met een vereenvoudigd cliëntenonderzoek. Dat is het geval indien uit de risicobeoordeling volgt dat een zakelijke relatie of transactie naar zijn aard een laag risico op witwassen of financieren van terrorisme met zich brengt.[82] Een instelling kan bij een vereenvoudigd cliëntenonderzoek volstaan met het treffen van vereenvoudigde cliëntenonderzoeksmaatregelen.

Een instelling zal in het geval van cliënten waarbij vereenvoudigd cliëntenonderzoek is toegepast in ieder geval over voldoende gegevens moeten beschikken om vast te stellen dat bij de cliënt kan worden volstaan met vereenvoudigd cliëntenonderzoek en om aan de verplichting tot het melden van ongebruikelijke transacties te voldoen.[83]

### Q&A

**QA3.5: Vraag**
Wat houdt een vereenvoudigd cliëntenonderzoek in?

**Antwoord**
De wet specificeert niet wat een vereenvoudigd cliëntenonderzoek inhoudt. De intensiteit van het cliëntenonderzoek kan afgestemd worden op het (lage) risico.[84]
Ook bij een vereenvoudigd cliëntenonderzoek moet worden voldaan aan art. 33 lid 2 Wwft. Ook moet een instelling kunnen voldoen aan de meldplicht van art. 16 Wwft.

---

**QA3.6: Vraag**
Moet altijd cliëntenonderzoek plaatsvinden?

**Antwoord**
Ja, er moet altijd cliëntenonderzoek worden uitgevoerd. Dit geldt ook in het geval dat er sprake is van een zodanig laag risico dat volstaan kan worden met een vereenvoudigd cliëntenonderzoek.[85]

82 Art. 6 lid 1 Wwft.
83 Art. 6 lid 2 en 4 jo. art. 16 lid 2 Wwft.
84 Kamerstukken II, 2017-2018, 34 808, nr. 3, p. 9.
85 Art. 5 lid 4 Wwft.

**QA3.7: Vraag**
Moet een instelling altijd een risicobeoordeling verrichten bij een potentieel laag risico?

**Antwoord**
Ja. De conclusie dat vereenvoudigd cliëntenonderzoek gepast is zal altijd op basis van een risicobeoordeling zijn. Er vindt dus in alle gevallen een risicobeoordeling plaats, vervolgens wordt de intensiteit van het cliëntenonderzoek afgestemd op het ingeschatte risico.

---

**QA3.8: Vraag**
Welke factoren geven een indicatie van een potentieel laag risico?

**Antwoord**
De instelling neemt in de risicobeoordeling in ieder geval de niet-limitatieve lijst van risicofactoren mee die genoemd is in bijlage II van de vierde anti-witwasrichtlijn.[86] Deze factoren geven een indicatie wanneer er sprake is van een potentieel lager risico. Overheidsinstellingen, zowel uit EU-lidstaten als derde landen die doeltreffende wetgeving en toezicht hebben op de bestrijding van witwassen en terrorisme financiering, kunnen bijvoorbeeld wijzen op een laag risico.
Nadere risicofactoren staan ook genoemd in de EBA 'ML/TF Risk Factors Guidelines'.[87]

**QA3.9: Vraag**
Kan bij beursgenoteerde cliënten altijd uitgegaan worden van een lager risico?

**Antwoord**
Nee. Een beursnotering kan een risicoverlagende factor zijn. Instellingen kunnen er niet zonder meer van uitgaan dat een beursgenoteerde cliënt altijd een lager risico meebrengt. Er kunnen ook andere cliëntgebonden risicofactoren aan de orde zijn. Een factor die relevant kan zijn is waar de instelling beursgenoteerd is, en wat het percentage is van het aandelenkapitaal dat vrij verhandelbaar is.
Ten aanzien van de locatie van beursnotering geldt bijvoorbeeld dat de EU-transparantieregels, en vergelijkbare regels, inzicht bieden in de eigendom van de aandelen, wat niet zonder meer hoeft te gelden voor andere landen. Daarnaast kunnen er ook niet-cliëntgebonden risicofactoren spelen, verband houdend met bijvoorbeeld het type product, dienst of transactie en geografische risicofactoren. Om in te schatten met welke mate van diepgang het cliëntenonderzoek kan worden uitgevoerd is het nodig om vooraf een risicoanalyse te maken.

---

**QA3.10: Vraag**
Kan bij cliënten die zelf als Wwft-instelling kwalificeren uitgegaan worden van een lager risico?

**Antwoord**
Dit kan een risicoverlagende factor zijn. De omstandigheid dat een cliënt zelf als Wwft-instelling kwalificeert, duidt echter niet zonder meer op een lager risico op witwassen of financieren van terrorisme.[88] Een instelling kan deze omstandigheid meewegen in de risicobeoordeling van de zakelijke relatie of incidentele transactie.

86 Art. 6 lid 1 Wwft.
87 EBA (2021), Guidelines on ML/TF Risk Factors.
88 Kamerstukken II 2017-2018, 34808, nr.3, p. 35.

### GP3.4: Good practice – Gebruik risicofactoren

Een instelling maakt op voorhand een inschatting in welke gevallen vereenvoudigd cliëntenonderzoek wordt toegepast. Dit wordt gedaan door middel van een vooraf uitgevoerde risicoanalyse, met inachtneming van risicofactoren, op basis waarvan de laagrisico cliënten worden geïdentificeerd. De instelling neemt onder meer cliëntgebonden risicofactoren, product-, dienst-, transactie- of leveringskanaalgebonden risicofactoren en geografische risicofactoren mee in deze risicoanalyse. De instelling stelt deze risicoanalyse bij op basis van de laatste inzichten die naar voren komen, bijvoorbeeld uit incidenten, FIU-meldingen, sectorbrede ontwikkelingen etc.

De instelling onderbouwt dat de betreffende zakelijke relatie of transactie naar haar aard een lager risico op witwassen of financieren van terrorisme met zich brengt, en legt dit vast.

### GP3.5: Good practice – Intensiteit maatregelen afstemmen op risico

Een instelling past op grond van haar risicoanalyse vereenvoudigd cliëntenonderzoek op bepaalde laag risico cliënten toe. In het verlengde daarvan worden ook de maatregelen in het kader van voortdurende controle van de zakelijke relatie minder intens toegepast. De instelling monitort deze groep cliënten via transactiemonitoring en sanctiescreening. De instelling maakt daarbij gebruik van referentiegroepen. Indien het transactiegedrag van een cliënt afwijkt van de referentiegroep, is dit aanleiding voor de instelling om de cliëntrelatie te reviewen en eventueel aanvullende informatie op te vragen. Zolang er geen sprake is van afwijkend gedrag, gaat de instelling niet over tot review van de cliëntrelatie.

### GP3.6: Good practice – Vaststellen laag risico

Een verzekeraar beschouwt een overlijdensrisicoverzekering met een premie van minder dan EUR 2.500 per jaar als laag risico, en heeft vastgesteld dat leveringskanaal, type cliënt en geografische locatie het risico niet negatief beïnvloeden. De verzekeraar past vervolgens een vereenvoudigd cliëntenonderzoek toe t.a.v. deze categorie.

## 3.4 Regulier cliëntenonderzoek

### 3.4.1 Identificatie van de cliënt en verificatie van de identiteit

Met het vaststellen van de identiteit van de cliënt en de verificatie daarvan verschaft de instelling zichzelf duidelijkheid en zekerheid over met wie zij zaken doet. Dit is een belangrijk vereiste voor de instelling om de risico's met betrekking tot de cliënt in te kunnen schatten.

Bij het identificeren verstrekt de cliënt gegevens over zijn identiteit. Dit is vormvrij. Bij het verifiëren van de identiteit gaat het om het vaststellen dat de opgegeven identiteit overeenkomt met de werkelijke identiteit. Aan de hand van documenten, gegevens of inlichtingen uit betrouwbare en onafhankelijke bron controleert de instelling de juistheid van de door de cliënt opgegeven identiteit.

Naast de cliënt zelf dienen ook de eventuele vertegenwoordigers van de cliënt te worden geïdentificeerd, en dient die identiteit te worden geverifieerd (zie daarover 3.4.3).

## Q&A

**QA3.11: Vraag**
Hoe wordt de identiteit van de cliënt geverifieerd?

**Antwoord**
De identiteit wordt geverifieerd aan de hand van documenten, gegevens of inlichtingen uit betrouwbare en onafhankelijke bron.[89] Art. 4 Uitvoeringsregeling Wwft geeft een overzicht van documenten op basis waarvan verificatie kan plaatsvinden. Dit overzicht is niet limitatief. Daarnaast moet worden voldaan aan art. 33 Wwft. Meer in het algemeen volstaan documenten niet om de identiteit van de cliënt te verifiëren, als van deze documenten niet vaststaat dat daaraan adequate identificatie en verificatie vooraf is gegaan. Het gaat dan bijvoorbeeld om studentenpassen, werknemerspassen en afschriften van bijvoorbeeld nuts- of telecombedrijven. Het staat namelijk niet vast dat daar een adequate identificatie en verificatie door een andere instelling aan vooraf is gegaan.

**QA3.12: Vraag**
Kan voor de verificatie van de identiteit van de cliënt een elektronisch identificatiemiddel (eID-middel) worden gebruikt?

**Antwoord**
Ja, mits het gebruikte eID-middel voldoende betrouwbaar is. Een eID-middel is voldoende betrouwbaar wanneer dit voldoet aan het betrouwbaarheidsniveau 'substantieel' of 'hoog'. Deze betrouwbaarheidsniveaus zijn gedefinieerd in de eIDAS-verordening.[90]

**QA3.13: Vraag**
In hoeverre volstaat een naam-nummer controle voor verificatie van de identiteit van de cliënt?

**Antwoord**
In de regel is naam-nummer controle, bijvoorbeeld door overmaking van 1 cent, niet voldoende voor de verificatie van de identiteit. Dit houdt in dat er naast deze bron nog gebruik gemaakt wordt van een of meer andere onafhankelijke en betrouwbare bronnen.

### GP3.7: Good practice – Vaststellen betrouwbare bronnen

Ten behoeve van de verificatie van de identiteit van cliënten heeft een instelling vastgelegd welke documenten, inlichtingen of gegevens voor haar acceptabel zijn, en waarom. De instelling heeft ook betrokken wat in het internationale verkeer gebruikelijk is.

De instelling heeft hierbij een risicobeoordeling gebruikt, waarbij rekening is gehouden met de hoog-risicolandenlijst van de Europese Commissie. Uit deze risicobeoordeling blijkt dat de instelling begrijpt welke bronnen betrouwbaar en onafhankelijk zijn. De instelling neemt als factor bij de beoordeling mee het feit dat bepaalde documenten al dan niet bij wet erkend zijn als identificatiemiddel in de staat van herkomst van de cliënt.

89 Art. 11 Wwft.
90 Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van richtlijn 1999/93/eg

### 3.4.2 Uiteindelijk belanghebbende (UBO) & Pseudo-UBO

De uiteindelijk belanghebbende (ultimate beneficial owner, UBO) is de natuurlijke persoon die de uiteindelijke eigenaar is van of zeggenschap heeft over een cliënt, dan wel de natuurlijke persoon voor wiens rekening een transactie of activiteit wordt verricht.[91] Personen die criminele gelden in het financiële systeem willen brengen dan wel personen die gelden willen aanwenden voor terroristische doelen kunnen zich verschuilen achter bijvoorbeeld een rechtspersoon of een complexe vennootschappelijke structuur. Het is daarom belangrijk dat instellingen weten met wie ze te maken hebben, inzicht hebben in de eigendoms- en zeggenschapsstructuur, en weten wie de cliënt aanstuurt en uiteindelijk profiteert van de dienstverlening.

#### Q&A

**QA3.14: Vraag**

Wordt van iedere juridische entiteit een UBO vastgesteld?

**Antwoord**

Ja, de Wwft verplicht instellingen om de UBO van een cliënt vast te stellen en om redelijke maatregelen te nemen om de identiteit van de UBO te verifiëren, met uitzondering van beursgenoteerde vennootschappen waarop reeds openbaarmakingsvereisten[92] van toepassing zijn en 100%-dochtermaatschappijen van dergelijke vennootschappen.[93]
De UBO is altijd een natuurlijke persoon. De in de Wwft vastgelegde norm is niet alleen relevant wanneer de cliënt een juridische entiteit is, zoals een besloten vennootschap of een stichting, of een juridische constructie zoals een trust, maar is ook relevant als de cliënt een natuurlijke persoon is over wie een andere natuurlijke persoon feitelijke zeggenschap heeft of voor wiens rekening een transactie of activiteit wordt verricht.

**QA3.15: Vraag**

Wanneer is inzicht in de eigendoms- en zeggenschapsstructuur van de cliënt nodig?

**Antwoord**

Een instelling moet redelijke maatregelen nemen om in het geval van rechtspersonen en andere juridische entiteiten, en trusts en andere juridische constructies inzicht te verkrijgen in de eigendoms- en zeggenschapsstructuur van de cliënt.[94] Daaronder vallen ook maatregelen om de juridische status van cliënten anders dan natuurlijke personen te verifiëren, waar mogelijk door middel van het verkrijgen van bewijs van het bestaan van de rechtspersoon.[95]
Het uitgangspunt is kortom dat de instelling de structuur van de cliënt kent en ook begrijpt.
De diepgang van het onderzoek daarnaar past bij de complexiteit en het risico.

91 Art. 1, lid 1 onder b Wwft.
92 Het gaat daarbij om openbaarmakingsvereisten zoals neergelegd in Richtlijn 2004/109/EG van het Europees Parlement en de Raad van 15 december 2004 betreffende transparantievereisten die gelden voor informatie over uitgevende instellingen waarvan effecten tot de handel op een gereglementeerde markt zijn toegelaten en tot wijziging van Richtlijn 2001/34/EG, PbEU 2004, L 390, of vergelijkbare openbaarmakingsvereisten van een staat buiten de Europese Unie; Stb. 2018, 241, p. 30.
93 Art. 3 lid 1 onder a Uitvoeringsbesluit Wwft 2018.
94 Art. 3, lid 2 onder b Wwft.
95 Basel Committee on Banking Supervision (2020), Guidelines. Sound Management of Risk Related to Money Laundering and Financing of Terrorism, annex 4.

**QA3.16: Vraag**
Wanneer kwalificeert een natuurlijk persoon als een UBO?

**Antwoord**
Art. 3 Uitvoeringsbesluit Wwft 2018 geeft een uitwerking van natuurlijke personen die in elk geval moeten worden aangemerkt als UBO. Hierin wordt afhankelijk van het type juridische entiteit aangegeven hoe de UBO's dienen te worden bepaald. Het uitvoeringsbesluit bevat onder meer regels voor BV's en NV's,[96] kerkgenootschappen,[97] overige rechtspersonen (waaronder stichtingen en verenigingen)[98] en personenvennootschappen (waaronder een Vennootschap onder Firma).[99]

Voor de meeste juridische entiteiten geldt op grond van het Uitvoeringsbesluit dat een natuurlijk persoon kwalificeert als UBO indien deze direct of indirect meer dan 25% van eigendom of zeggenschap heeft in/over de juridische entiteit. Ter illustratie: bij BV's en NV's zijn de UBO's de natuurlijke personen die de uiteindelijk eigenaar zijn van of zeggenschap hebben over de vennootschap via het direct of indirect houden van meer dan 25% van de aandelen, van de stemrechten of van het eigendomsbelang in de vennootschap.

De 25%-regel is indicatief bedoeld.[100] Ook personen met een lager percentage kunnen als UBO worden aangemerkt indien deze personen op andere wijze de uiteindelijke zeggenschap of eigendom hebben. Indien alle mogelijke middelen zijn uitgeput, en er geen gronden van verdenking bestaan, er geen UBO's zijn achterhaald of indien er twijfel bestaat of deze personen UBO's zijn op die gronden, dan worden de personen die behoren tot het hoger leidinggevend personeel van de rechtspersoon als UBO aangemerkt.[101]

96 Art. 3 lid 1 onder a Uitvoeringsbesluit Wwft 2018.
97 Art. 3 lid 1 onder b Uitvoeringsbesluit Wwft 2018.
98 Art. 3 lid 1 onder c Uitvoeringsbesluit Wwft 2018.
99 Art. 3 lid 1 onder d Uitvoeringsbesluit Wwft 2018.
100 Kamerstukken II 2017-2018, 34808, nr. 3, p. 4.
101 Art. 3 lid 1 Uitvoeringsbesluit Wwft 2018.

**QA3.17: Vraag**
Moeten er in alle gevallen identiteitsbewijzen opgevraagd worden om aan de verificatie-eis te kunnen voldoen?

**Antwoord**
Nee, dat is niet in alle gevallen nodig. De instelling neemt redelijke maatregelen om de identiteit van de UBO's te verifiëren. Zo kan het bij een vereenvoudigd cliëntenonderzoek bijvoorbeeld passend zijn om de cliënt te laten verklaren dat de uit het handelsregister blijkende UBO's daadwerkelijk de UBO's van de cliënt zijn en dat de opgegeven identiteit overeenkomt met de werkelijke identiteit. Instellingen dienen daarbij evenwel rekening te houden met de passendheid van de genomen maatregelen (zie ook QA3.18).

**QA3.18: Vraag**
Wat zijn 'redelijke maatregelen' om de identiteit van de UBO te verifiëren?

**Antwoord**
'Redelijke maatregelen' zijn maatregelen die passend zijn bij het risico. Weliswaar schrijft de Wwft niet dwingend voor welke informatiebronnen geschikt zijn voor de verificatie van UBO's, maar de gebruikte informatiebronnen moeten wel toereikend zijn voor het bereiken van het beoogde doel. Het gaat erom dat de instelling weet wie de UBO is en voldoende (passend bij het risico) betrouwbare informatie heeft over de identiteit van de UBO.

**QA3.19: Vraag**
Wat als er geen UBO's kunnen worden vastgesteld of er twijfel bestaat?

**Antwoord**
Een instelling is gehouden de dienstverlening te weigeren of te beëindigen als er geen UBO kan worden vastgesteld. Dan kan namelijk niet aan de vereisten van het cliëntenonderzoek worden voldaan.[102] Voor situaties waarin geen UBO kan worden vastgesteld op basis van eigendom of zeggenschap, bestaat de terugvaloptie van de pseudo-UBO: de natuurlijke personen die behoren tot het hoger leidinggevend personeel van de cliënt worden in dat geval aangemerkt als (pseudo-)UBO, mits aan bepaalde voorwaarden is voldaan. Dit is verder uitgewerkt in art. 3 Uitvoeringsbesluit Wwft 2018.

Het hoger leidinggevend personeel kan alleen dan als pseudo-UBO worden aangemerkt, indien alle mogelijke maatregelen door een instelling zijn ingezet om de UBO's van een cliënt vast te stellen en indien er geen gronden bestaan voor verdenking van witwassen of financieren van terrorisme. De instelling legt de genomen maatregelen en de ondervonden moeilijkheden tijdens het verificatieproces vast.[103]

### GP3.8: Good practice – Rol cliënt in complexe structuur

Een rechtspersoon die cliënt wil worden van een instelling is onderdeel van een grotere structuur. De moeder van deze rechtspersoon is gevestigd in een derde land, en heeft ook dochtervennootschappen in landen met een verhoogd risico.

De instelling onderzoekt waarom de groep waar de cliënt deel van uitmaakt gebruik maakt van deze complexe structuren. Hierbij bevraagt de instelling de cliënt over de ratio en de werking van de structuur. De instelling verlangt ook dat de cliënt een juridische en/of fiscale opinie over de werking van de structuur verstrekt.

Ook na onderzoek en na bestudering van de opinie(s) kan de instelling de rol van de potentiële cliënt in de structuur niet goed doorgronden. De instelling concludeert dat het cliëntenonderzoek niet naar behoren kan worden afgerond en besluit daarom de cliënt niet te accepteren.

### GP3.9: Good practice – Eenvoudige structuur

Een vennootschap die een slagerij drijft, heeft twee aandeelhouders. Dit zijn tevens de bestuurders. Dit blijkt uit de informatie uit het handelsregister en een bevestiging van die informatie door de cliënt. De aandeelhouders zijn broers van elkaar. De instelling heeft voldoende inzicht in de eigendoms- en zeggenschapsstructuur en merkt de broers aan als UBO.

### GP3.10: Good practice – UBO op grond van zeggenschap

Tijdens het cliëntenonderzoek blijkt dat de cliënt een grote financier heeft. Deze persoon is geen aandeelhouder en heeft geen stemrechten, maar heeft wel het recht om belangrijke beslissingen te blokkeren. De instelling merkt deze persoon op grond van zeggenschap aan als UBO, naast de reeds geïdentificeerde directeur-grootaandeelhouder.

102 Stb. 2018, nr. 241, p. 29 (Uitvoeringsbesluit Wwft 2018).
103 Art. 3 lid 2 onder b Wwft.

## GP3.11: Good practice – Risicogebaseerde invulling

Bij een cliënt met een laag risico heeft de instelling de gegevens uit het UBO-register opgevraagd, en legt dit ter verificatie voor aan de cliënt. De cliënt bevestigt dat de uit het register blijkende UBO's daadwerkelijk de UBO's van de cliënt zijn en dat de opgegeven identiteit overeenkomt met de werkelijke identiteit. De instelling heeft geen aanleiding om dit in twijfel te trekken. Hiermee zijn identificatie en verificatie van de UBO's voltooid.

In geval van een cliënt met een hoog risico neemt de instelling aanvullende maatregelen om de identiteit van de UBO's te verifiëren, bijvoorbeeld verificatie door middel van een gewaarmerkte kopie van een identiteitsdocument of aan de hand van een voldoende betrouwbaar elektronisch identificatiemiddel.

## GP3.12: Good practice – Pseudo-UBO bij laag risico

De instelling heeft vastgesteld dat er sprake is van een laag-risico situatie.
Op grond van eigendom en (feitelijke) zeggenschap kan de instelling geen UBO bepalen en identificeert daarom de leden van het hoger leidinggevend personeel van de cliënt als (pseudo-) UBO's. Hiertoe legt de instelling de gegevens uit het handelsregister, waaruit het hoger leidinggevend personeel blijkt, voor aan de cliënt. De cliënt bevestigt dat de uit het register blijkende personen daadwerkelijk het hoger leidinggevend personeel van de cliënt zijn en dat de opgegeven identiteit overeenkomt met de werkelijke identiteit. De instelling heeft geen aanleiding hieraan te twijfelen. Hiermee zijn identificatie en verificatie van de identiteit van de pseudo-UBO's voltooid. De instelling legt de genomen maatregelen en de ondervonden moeilijkheden tijdens het verificatieproces vast.

## GP3.13: Good practice – Pseudo-UBO bij hoog risico

De instelling heeft vastgesteld dat er sprake is van een hoog risico situatie, maar dat er geen gronden bestaan voor verdenking van witwassen of financieren van terrorisme.

De instelling kan op grond van eigendom en (feitelijke) zeggenschap geen UBO bepalen en identificeert daarom de pseudo-UBO's aan de hand van de gegevens uit het handelsregister.
De instelling verzoekt de cliënt daarnaast om een opgave van het hoger leidinggevend personeel. De verificatie van de identiteit van de betreffende natuurlijke personen vindt plaats aan de hand van een identiteitsdocument. De instelling legt de genomen maatregelen en de ondervonden moeilijkheden tijdens het verificatieproces vast.

## GP3.14: Good practice – Optellen van belangen

Een cliënt is onderdeel van een grotere structuur. De instelling ziet dat geen van de directe aandeelhouders meer dan 25% van de aandelen heeft. Bij het inzichtelijk maken van de structuur merkt de instelling op dat er enkele personen zijn die via meerdere vennootschappen een belang hebben. Na optelling blijkt dat er twee natuurlijke personen zijn die uiteindelijk een belang hebben van meer dan 25%. De instelling identificeert deze personen als UBO.

### GP3.15: Good practice – Onderzoek naar UBO's

Een cliënt heeft een uitgebreide structuur met meerdere lagen. Enkele van haar aandeelhouders zijn in hoog-risico jurisdicties gevestigd. Gezien de geïdentificeerde risico's van deze cliëntrelatie vindt de instelling een eigen opgave van de UBO's niet afdoende. De instelling neemt redelijke maatregelen om de eigendomsstructuur in kaart te brengen (bijvoorbeeld met behulp van uittreksels uit handelsregisters en aanvullende bronnen) en identificeert aan de hand daarvan drie personen met ieder indirecte formele zeggenschap van meer dan 25% als UBO. Vervolgens verifieert de instelling de identiteit van de UBO's door middel van een gewaarmerkte kopie van een identiteitsdocument. De instelling legt de uitkomsten (te weten de bronnen, analyse en conclusies) van het onderzoek vast in het cliëntendossier.

### GP3.16: Good practice – Hoog risico en minderheidsaandeelhouders

Een cliënt wordt op grond van verschillende aanwezige risicofactoren, waaronder risico's gelinkt aan de cliëntstructuur, als hoog risico geclassificeerd. De instelling besluit daarop verscherpt clientonderzoek uit te voeren en doet daarom nader onderzoek naar de zeggenschap van aandeelhouders in de structuur met een eigendomspercentage onder de 25%. Op basis van dat onderzoek concludeert de instelling, in overeenstemming met haar eigen beleid, dat ook bepaalde aandeelhouders met een lager eigendomspercentage UBO zijn. Zij past op deze aandeelhouders een PEP-screening toe.

### GP3.17: Good practice – Beleid validatie complexe structuren

Een instelling die overwegend te maken heeft met complexe (internationale) eigendoms- en zeggenschapsstructuren heeft beleid opgesteld waarin is vastgelegd in welke gevallen een interne of externe (fiscale) expert opinie gevraagd moet worden ten aanzien van een structuur.

### GP3.18: Good practice – Beleid identificatie en verificatie UBO EU-cliënten

Een instelling heeft in haar beleid het volgende opgenomen met betrekking tot cliënten in de EU:
Voor cliënten die classificeren als 'low risk' of 'neutral risk' kan verificatie van de identiteit van de UBO plaatsvinden aan de hand van een verklaring van de correspondentbank in een EU-lidstaat, met een door de correspondentbank ondertekende kopie van een identiteitsbewijs.
Voor cliënten die classificeren als 'high risk' kan verificatie van de identiteit van de UBO plaatsvinden aan de hand van een verklaring van een notaris met een gewaarmerkte kopie van een identiteitsbewijs.

### 3.4.3 Vertegenwoordiging en stromanrisico

Een natuurlijke persoon kan optreden als vertegenwoordiger van een cliënt. De Wwft verplicht om vast te stellen of deze persoon vertegenwoordigingsbevoegd is.[104] Als dit het geval is, kan de instelling verdergaan met het cliëntenonderzoek.

Daarnaast is het is van belang om vast te stellen of een natuurlijke persoon die zich presenteert als cliënt voor zichzelf optreedt of voor een ander.[105] Dit bepaalt wie de cliënt is.

104 Art. 3 lid 2 onder e Wwft.
105 Art. 3 lid 2 onder f Wwft.

## Q&A

**QA3.20: Vraag**
Moet de instelling vaststellen of de vertegenwoordiger ook bevoegd is?

**Antwoord**
Tijdens het cliëntenonderzoek stelt de instelling vast of de natuurlijke persoon die de cliënt vertegenwoordigt daartoe bevoegd is.[106] Dit geldt bijvoorbeeld waar een natuurlijke persoon optreedt als bestuurder van een rechtspersoon.[107]

---

**QA3.21: Vraag**
Geldt vertegenwoordiging alleen in geval van rechtspersonen?

**Antwoord**
Nee, iemand kan ook optreden als vertegenwoordiger van een natuurlijk persoon.

---

**QA3.22: Vraag**
In hoeverre moet de instelling de vertegenwoordiger identificeren en diens identiteit verifiëren?

**Antwoord**
In voorkomend geval identificeert de dienstverlener de natuurlijke persoon en verifieert diens identiteit.[108]

**VQA3.23: Vraag**
Waar moet een instelling extra alert op zijn?

**Antwoord**
Tijdens het cliëntenonderzoek gaat de instelling na of een persoon die zich presenteert als cliënt voor zichzelf optreedt of voor een ander.[109] Hierdoor kan de instelling ook nagaan of er sprake is van de inzet van een zogenoemde stroman, die handelt ten behoeve van (criminele) derden.
Als het duidelijk is dat iemand ten behoeve van een andere persoon handelt, dan kwalificeert deze andere persoon als cliënt – en moet dus cliëntenonderzoek worden gedaan naar die persoon.

---

**QA3.24: Vraag**
In hoeverre moet de instelling nagaan of er sprake is van een stroman?

**Antwoord**
De Wwft vereist dat instellingen redelijke maatregelen treffen waarmee kan worden vastgesteld of de cliënt voor zichzelf optreedt dan wel ten behoeve van een ander.110 Instellingen kunnen hun inspanningen concentreren op gevallen waar sprake lijkt van een verhoogd 'stromanrisico' – dus een risicogebaseerde aanpak hanteren.

106 Art. 3 lid 2 onder e Wwft.
107 Kamerstukken II 2011-2012, 33238, nr. 3, p. 13.
108 Art. 3 lid 2 onder e Wwft.
109 Art. 3 lid 2 onder f Wwft.
110 Art. 3 lid 2 onder f Wwft

### GP3.19: Good practice – Keten van vertegenwoordigingsbevoegdheid

Bij een rechtspersoon zijn de vertegenwoordigers vaak de bestuurders. Wanneer een natuurlijk persoon stelt dat hij indirect een rechtspersoon vertegenwoordigt, wordt ook de keten van vertegenwoordigingsbevoegdheid vastgesteld. Dit kan bijvoorbeeld door uittreksels uit het handelsregister en statuten op te vragen.

### GP3.20: Good practice – Stromanrisico

Een instelling stelt indicatoren op die wijzen op een 'stromanrisico' en die worden toegepast in het cliëntenonderzoek. Te denken valt aan gevallen dat de persoon bepaalde vragen niet kan beantwoorden, zoals over de herkomst van het geld, of wanneer er onduidelijke, vage redenen voor de transactie worden gegeven.

Indien de instelling vermoedt dat de cliënt een stroman is, wordt dit behandeld als een verhoogd of onacceptabel risico. Als het duidelijk is dat een cliënt ten behoeve van een andere (natuurlijk of rechts-)persoon handelt, dan kwalificeert de instelling deze andere persoon ook als cliënt en gelden de verplichtingen ten aanzien van het cliëntenonderzoek ook ten aanzien van deze persoon.

## 3.4.4 Doel en aard van de zakelijke relatie

Met het vaststellen van doel en aard van de zakelijke relatie heeft de instelling inzicht in waarom en waarvoor de cliënt de dienstverlening wil gebruiken. Het vaststellen van het doel en de beoogde aard van de zakelijke relatie ondersteunt de instelling bij het inschatten van risico's van de dienstverlening aan de cliënt.

### Q&A

**QA3.25: Vraag**

Moet een instelling in alle gevallen doel en aard van de zakelijke relatie vaststellen?

**Antwoord**

Ja. De Wwft bepaalt dat het cliëntenonderzoek de instelling in staat dient te stellen om het doel en de aard van de zakelijke relatie vast te stellen.[111] De intensiteit van het onderzoek stemt de instelling af op het risico van de cliënt met betrekking tot witwassen en financieren van terrorisme.

---

**QA3.26: Vraag**

In hoeverre kunnen doel en aard van de zakelijke relatie worden vastgesteld aan de hand van de afgenomen producten?

**Antwoord**

Het vaststellen van het doel en de beoogde aard van de zakelijke relatie stelt een instelling in staat om eventuele risico's die de dienstverlening aan een cliënt oplevert in te schatten. De benodigde informatie voor het vaststellen van doel en aard zal doorgaans al naar voren komen tijdens het contact voorafgaand aan de zakelijke relatie.

Doel en aard van de zakelijke relatie kunnen –met inachtneming van de kenmerken van de betreffende cliënt - blijken uit de afgenomen diensten of producten, bijvoorbeeld:

- rekening-courant voor het afhandelen van reguliere betalingstransacties (privé/zakelijke rekening)
- levensverzekeringsproducten
- traditionele beleggingsproducten voor vermogensbescherming/vermogensopbouw
- effectenrekeningen.

111 Art. 3 lid 2 onder c Wwft.

Indien doel en aard niet afdoende blijken uit de afgenomen diensten en/of producten wordt aanvullende informatie verzameld.

**QA3.27: Vraag**
Kunnen doel en aard van de zakelijke relatie worden vastgesteld m.b.v. peer grouping?

**Antwoord**
Ja. Doel en aard van de zakelijke relatie worden vastgesteld met het oog op het inschatten van de risico's. Een instelling kan haar zakelijke relaties indelen naar referentiegroepen ('peer groups'). Voor bepaalde referentiegroepen kunnen doel en aard van de relatie voldoende duidelijk zijn.

### GP3.21: Good practice – Bevragen cliënt bij onduidelijkheid
Het is voor een instelling die met name de Nederlandse markt bedient, niet duidelijk waarom een cliënt die niet in Nederland gevestigd of woonachtig is, diensten of producten bij haar afneemt. De instelling bevraagt de cliënt hierover, en beoordeelt wat dit betekent voor het risicoprofiel en of dit risico voor haar acceptabel is.

### GP3.22: Good practice – Intensiteit bij hogere risico's
Naast de zakelijke relaties of transacties die op grond van de risicobeoordeling een hoger risico op witwassen of financieren van terrorisme meebrengen, kan een hoog risico ook ontstaan omdat de cliënt woonachtig of gevestigd is of zijn zetel heeft in een (derde) hoog risicoland, er sprake is van een PEP of van een correspondentrelatie.

In dat geval brengt de instelling in kaart wat voor soort transacties de cliënt zal verrichten. De instelling kijkt daarbij naar de aard, hoeveelheid, frequentie en grootte van de transacties en met welke landen of gebieden de cliënt transacties verricht. Dit bepaalt mede de aard van de relatie. De instelling beoordeelt wat dit betekent voor het risicoprofiel en of, en onder welke voorwaarden, dit risico voor haar acceptabel is.

### GP3.23: Good practice – Gebruik van referentiegroepen
Een instelling met een groot aantal cliënten maakt gebruik van referentiegroepen. De instelling heeft referentiegroepen gedefinieerd aan de hand van een aantal cliëntkenmerken. Bij cliënten die niet in een referentiegroep vallen, wint de instelling nadere informatie in over onder meer doel en aard van de zakelijke relatie, waarbij de instelling ook meer inzicht krijgt in wat voor soort transacties de cliënt zal verrichten.

### GP3.24: Good practice – Aanvullende informatie
In het geval van verscherpte onderzoeksmaatregelen bij een hoger risico, verzamelt de instelling aanvullende informatie (zoals informatie over het soort transacties dat de cliënt zal verrichten, het volume daarvan en de activiteiten van de cliënt). Mede op basis hiervan stelt de instelling doel en aard van de relatie vast.

### 3.4.5 Bron van de middelen

Het vaststellen van de bron van de middelen, die bij de zakelijke relatie of transactie worden gebruikt, draagt bij aan het inzicht dat de instelling heeft in de risico's van de dienstverlening aan de cliënt. Deze risico's hebben onder meer betrekking op het risico dat mogelijk criminele geldstromen door de instelling worden gefaciliteerd.

### Q&A

**QA3.28: Vraag**

Moet een instelling in alle gevallen de bron van de middelen vaststellen?

**Antwoord**

Nee. De instelling verricht zo nodig een onderzoek naar de bron van de middelen die bij de zakelijke relatie of de tijdens de duur van deze relatie verrichte transactie gebruikt worden.[112] Of het nodig is om een dergelijk onderzoek te doen, is afhankelijk van de inschatting die de instelling maakt van het risico.[113] De Wwft schrijft twee situaties voor waarin in ieder geval onderzoek dient te worden gedaan naar de bron van de middelen:

- Bij transacties, zakelijke relaties en correspondentrelaties, gerelateerd aan staten die door de Europese Commissie zijn geïdentificeerd als jurisdicties met een hoger risico op witwassen en financieren van terrorisme, onderzoekt de instelling de bron van de middelen. Instellingen verzamelen in zulke gevallen informatie over de herkomst van de fondsen die bij de zakelijke relatie of transactie worden gebruikt en de bron van het vermogen van cliënten en UBO's.[114] Instellingen vullen deze verplichting risicogebaseerd in.[115]
- Daarnaast moet een instelling bij het aangaan of voorzetten van een zakelijke relatie met, of het verrichten van een transactie voor, een PEP passende maatregelen treffen om de bron van het vermogen en van de middelen die bij deze zakelijke relatie of deze transactie gebruikt worden, vast te stellen.[116]

**QA3.29: Vraag**

In hoeverre moet de instelling onderzoek doen naar de bron van de middelen als inkomende gelden afkomstig zijn van een gereguleerde instelling?

**Antwoord**

Dat gelden afkomstig zijn van een gereguleerde instelling kan een risicoverlagende factor zijn, maar dat betekent niet dat de instelling geen zelfstandig onderzoek hoeft uit te voeren. Afhankelijk van de geïdentificeerde risico's bepaalt de instelling of een onderzoek naar de bron van de middelen nodig is.[117]

112 Art. 3 lid 2 onder d. Wwft.
113 Kamerstukken II 2011-2012, 33 238, nr. 3, p. 12.
114 Art. 9 lid 1 onder c Wwft.
115 Kamerstukken II 2018-2019, 35 245, 3, p. 30. EBA (2021), Guidelines on ML/TF Risk Factors, par. 4.53-4.54.
116 Art. 8 lid 5 onder b sub 2 Wwft.
117 Zie art. 3 lid 8 en 9 Wwft en bijlage I vierde anti-witwasrichtlijn over het afstemmen van het cliëntenonderzoek aan de hand van diverse factoren op de risicogevoeligheid voor ML/TF.

**QA3.30: Vraag**
In hoeverre moet de herkomst van het gehele vermogen van de cliënt worden onderzocht?

**Antwoord**
Het uitgangspunt is dat de bron van de middelen die worden aangewend in de relatie of de transactie wordt onderzocht. [118] De overige bestanddelen van het vermogen van de cliënt kunnen dan buiten beschouwing blijven. Afhankelijk van het risico kan het nodig zijn om dieper onderzoek te doen naar de bron van de middelen.

In het geval van cliënten en UBO's die kwalificeren als PEP of die gerelateerd zijn aan staten die door de Europese Commissie zijn aangewezen als staten met een hoger risico op witwassen of financieren van terrorisme moeten instellingen passende maatregelen nemen om de bron van de middelen en het vermogen vast te stellen, of informatie verzamelen over de herkomst van de fondsen en de bron van het vermogen.[119]

### GP3.25: Good practice – Gebruik van indicatoren voor diepgang onderzoek
De instelling identificeert indicatoren op basis waarvan de diepgang van het onderzoek wordt bepaald om de plausibiliteit van de (legale) bron van de middelen vast te stellen. Enkele combinaties van indicatoren die de instelling gebruikt, zijn het betreffende bedrag, de opgegeven bron van de middelen, leeftijd en beroep of bedrijfsactiviteiten van de cliënt, land van herkomst of bestemming van de middelen en de geleverde producten of diensten.

### GP3.26: Good practice – Beleid en vastlegging onderzoek bron van middelen
Een instelling gaat bij hoge stortingen die buiten het risicoprofiel van de client vallen na wat de bron van de middelen is. Daarnaast wordt bij alle cliënten die als hoog risico worden gekwalificeerd de bron van de middelen onderzocht aan de hand van onafhankelijke, betrouwbare bronnen. De instelling legt het onderzoek, de bewijsstukken en de conclusie vast in het cliëntendossier.

### GP3.27: Good practice – Bewijsstukken bron van middelen
Bij het onderzoek naar de bron van de middelen gebruikt de instelling onafhankelijke, betrouwbare bronnen. Afhankelijk van het risico maakt de instelling onder meer gebruik van (gewaarmerkte kopieën van) loonstroken, werkgeversverklaringen, een verkoopcontract, overzichten van aandelenposities, testamenten, jaarrekeningen, belastingaangiften.

### GP3.28: Good practice - Huurpenningen
Een cliënt wil een zakelijke rekening openen bij een bank. De cliënt wil de rekening gebruiken voor het ontvangen van huurpenningen. Navraag leert dat de cliënt een aantal kantoorpanden bezit, die hij verhuurt.

In het kader van het onderzoek naar de bron van de middelen wil de bank weten of het bezit van de kantoorpanden past bij de achtergrond van deze cliënt – de bank onderzoekt op dit punt de bron van het vermogen om zodoende beter zicht te krijgen op de bron van de middelen die bij de bank binnenkomen.

118 Kamerstukken II 2011-2012, 33 238, nr. 3, p. 12.
119 Art. 8 lid 5 onder b sub 2 Wwft. Art. 9 lid 1 onder c Wwft. Zie ook Kamerstukken II 2017-2018, 34 808, 3, p. 55-56.

## 3.5 Omgang met politiek prominente personen (PEP)

Een PEP is een persoon die een prominente publieke functie bekleedt of heeft bekleed.
Vanwege de potentiële corruptie- en reputatierisico's die verbonden zijn aan de PEP, vereist de Wwft bijzondere aandacht voor deze personen.[120]

PEP's brengen niet zonder meer een hoog risico op witwassen of financieren van terrorisme mee.[121]
Risicoverhogende factoren die verbonden kunnen zijn aan een PEP zijn bijvoorbeeld de toegang tot grote publieke fondsen, controle over staatsbedrijven en –contracten, en mogelijkheden om overheidsgeld in door hen gecreëerde structuren onder te brengen.[122]
Het is daarom van belang dat instellingen weten of hun cliënt of de UBO van de cliënt een PEP is. Met die kennis kan de instelling de risico's met betrekking tot de cliënt beter vaststellen.

### Q&A

**QA3.31: Vraag**
Wie kwalificeren er als PEP?

**Antwoord**
Een PEP wordt gedefinieerd als een natuurlijke persoon die een prominente publieke functie bekleedt of heeft bekleed. Onder een PEP worden ook verstaan familieleden of naaste geassocieerden van deze persoon.[123] Art. 2 lid 1 Uitvoeringsbesluit Wwft 2018 geeft een nadere uitwerking van wat beschouwd wordt als prominente publieke functie, als familierelaties van de PEP en wie beschouwd worden als naaste geassocieerde.[124]

---

**QA3.32: Vraag**
Vormen alle PEP's een hoog risico?

**Antwoord**
Nee. Hoewel de Wwft ervan uitgaat dat PEP's in de basis een verhoogd risico vertegenwoordigen, is er bij een PEP niet altijd sprake van een hoog risico. Dit is afhankelijk van meer factoren dan alleen de PEP-status.[125]

120 Kamerstukken II 2007-2008, 31 238, nr. 3, p. 21-22.
121 FATF (2012), Specific Risk Factors in Laundering the Proceeds of Corruption. Assistance to Reporting Institutions, p. 4.
122 FATF (2011), FATF Report Laundering the Proceeds of Corruption.
123 Art. 1 lid 1 Wwft.
124 De Belastingdienst heeft een lijst gepubliceerd van prominente publieke functies. Dit is de uitwerking van art. 2 Uitvoeringsbesluit Wwft 2018.
Zie: https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/wwft-prominente-publieke-functies.
125 FATF (2013), FATF Guidance. Politically Exposed Persons (Recommendations 12 and 22). In dat kader kan het van pas komen om te weten wat het corruptieniveau is in het land waar de persoon de functie bekleedt. Hiertoe kan bijvoorbeeld de Corruption Perception Index van Transparency International worden gebruikt.

Zo zijn kinderen van een Kamerlid in Nederland met een eenvoudige betaalrekening in potentie minder risicogevoelig dan de echtgenote van een staatshoofd van een land met een verhoogd corruptierisico, die een private bankrekening opent.

**QA3.33: Vraag**
Welke aanvullende maatregelen zijn verplicht met betrekking tot een PEP?

**Antwoord**
De volgende aanvullende maatregelen zijn verplicht bij een PEP:[126]

- Voor het aangaan of voortzetten van de zakelijke relatie of het verrichten van de transactie, is de toestemming vereist van een persoon die deel uitmaakt van het hoger leidinggevend personeel van de instelling.[127]
- Instellingen nemen passende maatregelen om de bron van het vermogen en van de middelen die bij de zakelijke relatie of de transactie gebruikt worden vast te stellen.
- De zakelijke relatie wordt doorlopend aan verscherpte controle onderworpen.

Instellingen kunnen de intensiteit van de maatregelen en de diepgang van de uit te voeren onderzoeken afstemmen op het risicoprofiel van de cliënt of de UBO. De aanvullende maatregelen kunnen echter niet volledig achterwege worden gelaten.

**QA3.34: Vraag**
Vervalt de PEP-status nadat de persoon niet meer onder de PEP-definitie valt?

**Antwoord**
Indien de cliënt of de UBO niet langer een prominente publieke functie bekleedt, past de instelling passende risicogebaseerde maatregelen zo lang als nodig, doch ten minste gedurende 12 maanden toe, totdat deze persoon niet langer het hoger risico met zich brengt dat hoort bij PEP's.[128]

**QA3.35: Vraag**
Wat als de cliënt gedurende de zakelijke relatie een PEP wordt of blijkt te zijn?

**Antwoord**
Indien de cliënt of de UBO gedurende de zakelijke relatie een PEP wordt of blijkt te zijn (of een familielid of naaste geassocieerde), neemt de instelling onverwijld nadat hiervan is gebleken de vereiste maatregelen.[129]

126 Art. 8 lid 5 Wwft.
127 Art. 1 lid 1 Wwft: hoger leidinggevend personeel: a. personen die het dagelijks beleid van een instelling bepalen; of b. personen werkzaam onder verantwoordelijkheid van een instelling, die een leidinggevende functie vervullen direct onder het echelon van de dagelijks beleidsbepalers en die verantwoordelijk zijn voor natuurlijke personen wier werkzaamheden van invloed zijn op de blootstelling van een instelling aan de risico s op witwassen en het financieren van terrorisme.
128 Art. 8 lid 7 Wwft.
129 Art. 8 lid 9 Wwft.

## GP3.29: Good practice – PEP-screening

Een instelling beoordeelt bij cliëntacceptatie en doorlopend of haar cliënt én de UBO's kwalificeren als PEP. De instelling combineert deze PEP-controle met andere doorlopende screenings, zoals het ophalen van eventuele nadelige mediaberichtgeving over een cliënt. Indien blijkt dat een cliënt of UBO na verloop van tijd kan worden aangemerkt als PEP, brengt de instelling allereerst het risico in kaart. Vervolgens neemt de instelling de voor de PEP geldende en passende maatregelen.

## GP3.30: Good practice – Meerdere methoden om PEP te bepalen

Een instelling gebruikt de volgende methoden om te onderzoeken of een persoon kwalificeert als PEP:

- Screening tegen beschikbare PEP-lijsten.
- Naast het gebruik van algemene PEP-lijsten ook een screening tegen eigen 'lokale' PEP-lijsten. Met behulp daarvan voert de instelling ook een controle uit op namen van lokale individuen belast met prominente functies.
- Onderzoek doen op het internet, bijvoorbeeld naar het bestuur in het herkomstland van de cliënt via het lokale handelsregister.
- Om tijdens het CDD-proces voldoende informatie te verzamelen voor het identificeren van PEP's hanteert de instelling een gerichte vragenlijst, ook om te achterhalen of er sprake is van een familielid of een naaste geassocieerde die kwalificeert als PEP.

## GP3.31: Good practice – PEP en complexe structuren

Alleen een check tegen een PEP-lijst voldoet niet in elke situatie. De instelling is zich ervan bewust dat een PEP zich kan verschuilen achter een andere persoon (verhullings- of stromanrisico). Bij complexe structuren verricht de instelling aanvullende inspanningen om deze te doorgronden en om de UBO vast te stellen. De instelling heeft daarbij niet alleen aandacht voor 'eigendom' maar ook voor 'zeggenschap'.

De compliancefunctie verricht gerichte controles op de werking en effectiviteit van procedures voor het vaststellen van PEP's.

## GP3.32: Good practice – Actuele PEP-lijsten

Een instelling voert periodiek een audit uit of voor de PEP-screening alle relevante lijsten worden gebruikt en actueel zijn. Voor actualisatie van de gebruikte PEP-lijsten wordt onder meer gebruik gemaakt van een abonnement bij een externe dienstverlener. De instelling actualiseert de lokale PEP-lijst na gebeurtenissen als verkiezingen of een bestuurswissel.

## GP3.33: Good practice – Gebruik 'red flags'

Bij het beoordelen van het risico ten aanzien van een PEP hanteert de instelling een aantal factoren of 'red flags'. De instelling vindt het risico hoger als de volgende situaties zich voordoen:

- De PEP komt uit een jurisdictie met een hoger risico op witwassen en/of corruptie, of uit een door de EU of VN gesanctioneerd land.
- Er is negatief nieuws over de PEP, inclusief negatieve jurisprudentie.
- De beschikbare informatie over de cliënt (beroep, leeftijd, inkomen) past niet goed bij informatie over de bron van middelen en vermogen.
- De cliënt/UBO verschaft documenten over de bron van middelen en vermogen die inconsistent zijn met dat wat vergelijkbare cliënten aanleveren.
- De cliënt/UBO verschaft documenten over de bron van middelen en vermogen afkomstig uit hoog risico jurisdicties.

- De cliënt/UBO verschaft documenten over de bron van middelen en vermogen die gebrekkig zijn of waar de rationale van ontbreekt.
- De cliënt/UBO verschaft informatie over de bron van middelen en vermogen via complexe, ondoorzichtige structuren (bijvoorbeeld offshore structuren, trusts, bankrekeningen in hoogrisicolanden), en de informatie blijft onduidelijk.

De instelling neemt in deze situaties aanvullende beheersmaatregelen, zoals: het stellen van aanvullende vragen, het stellen van grenzen aan transactiebedragen en het vooraf beoordelen van transacties die de PEP wil doen. De instelling overweegt in deze situaties of het risico nog acceptabel is en of het cliëntenonderzoek naar behoren kan worden afgerond. Zo niet dan weigert, beëindigt of beperkt de instelling de dienstverlening.

### GP3.34: Good practice – Oog voor de client

Een instelling vult het verscherpte cliëntenonderzoek risicogebaseerd in, met daarbij oog voor de potentiële belasting voor de cliënt en voor de medewerker. De instelling ziet ook de mogelijke weerstand onder ogen vanuit een medewerker of vanuit een cliënt die niet begrijpt waarom bepaalde informatie moet worden aangeleverd. De instelling legt daarom, zowel intern aan haar medewerkers als extern richting haar cliënten in begrijpelijke taal uit waarom bepaalde informatie wordt opgevraagd.

### GP3.35: Good practice – Betrokkenheid hoger leidinggevend personeel

Het hoger leidinggevend personeel van een instelling speelt niet alleen een rol bij het goedkeuren van een relatie of transactie, maar laat zich periodiek informeren over de exposure t.a.v. PEP's, en geeft hierop al dan niet akkoord.

Verder kijkt Compliance actief mee bij de acceptatie van cliënten waar een PEP bij betrokken is en geeft zij advies over de acceptatie. Compliance betrekt daarbij de totale 'PEP-exposure' en het daadwerkelijke risico dat de instelling kan lopen bij acceptatie. Compliance heeft de middelen en de positie om daarin onafhankelijk te opereren en adviseren. Het advies van Compliance over het risico wordt zwaarwegend meegewogen door het hoger leidinggevend personeel in de beslissing over de relatie.

## 3.6 Omgang met hoogrisicolanden

De FATF en de Europese Commissie wijzen regelmatig op jurisdicties die tekortkomingen hebben in hun systeem ter bestrijding van witwassen en terrorismefinanciering. Het onderhouden van zakelijke relaties met ingezetenen van deze jurisdicties of het uitvoeren van transacties van of naar deze jurisdicties kan een hoger risico op witwassen en terrorismefinanciering meebrengen. Het is daarom van belang dat instellingen verhoogde aandacht geven aan de zakelijke relaties en transacties gerelateerd aan de hoog risicolanden (ook bekend als *High Risk Third Countries*, HRTC), waaronder het uitvoeren van verscherpt cliëntenonderzoek.[130]

130 Art. 8 lid 1 sub b en art. 9 Wwft.

## Q&A

**QA3.36: Vraag**
Wat is volgens de Europese Commissie een staat met hoog risico op witwassen en financieren van terrorisme?

**Antwoord**
De Europese Commissie wijst landen aan die in hun nationale regelgeving strategische tekortkomingen vertonen die een aanzienlijke bedreiging vormen voor het financiële stelsel van de Unie (*High Risk Third Countries*, HRTC).[131]
Deze landen worden op een lijst geplaatst. Deze lijst is te vinden in de gedelegeerde verordening (EU) 2016/1675 van de Commissie tot aanvulling van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad door de identificatie van derde landen met een hoog risico die strategische tekortkomingen vertonen. De lijst wordt geregeld bijgewerkt.

---

**QA3.37: Vraag**
In welke mate doet een instelling bij elke transactie gerelateerd aan een HRTC verscherpt onderzoek?

**Antwoord**
Op basis van art. 9 Wwft moet een instelling met betrekking tot transacties, zakelijke relaties en correspondentbankrelaties gerelateerd aan HRTC verplicht een aantal verscherpte onderzoeksmaatregelen uitvoeren. De intensiteit van deze maatregelen kan per geval variëren aan de hand van het geïdentificeerde risico, bijvoorbeeld ten aanzien van het verzamelen van aanvullende informatie. In ieder geval wordt van een instelling verwacht dat deze beargumenteerd kan toelichten waarom in een bepaald geval een lagere mate van intensiteit is toegepast.

**QA3.38: Vraag**
Welke maatregelen moet een instelling toepassen bij zakelijke relaties en transacties gerelateerd aan een HRTC?

**Antwoord**
Art. 9 lid 1 Wwft geeft een overzicht van de verscherpte onderzoeksmaatregelen. Dit betreft onder meer het verzamelen van informatie over de achtergrond van de voorgenomen of verrichte transacties van die cliënten en het verkrijgen van goedkeuring van het hoger leidinggevend personeel voor het aangaan of voortzetten van de zakelijke relatie.

---

**QA3.39: Vraag**
Moet een instelling bij een transactie gerelateerd aan een HRTC altijd de cliënt benaderen voor aanvullende informatie?

**Antwoord**
Nee. In het kader van de risicogebaseerde benadering kan de instelling in bepaalde gevallen aanvullende informatie op basis van eigen deskresearch of openbare bronnen verzamelen, zonder direct contact op te nemen met de cliënt.

- Zo bevat het cliëntendossier informatie (o.a. over identiteit, bron van middelen). Deze informatie hoeft niet opnieuw opgevraagd te worden indien deze actueel is, tenzij er bijvoorbeeld sprake is van een situatie die niet past in het profiel zoals dat uit het cliëntendossier blijkt.
- Bepaalde informatie (bijvoorbeeld over de aard van de transactie) kan de instelling vaststellen door analyse van transactiedata en/of openbare bronnen.

131 Art. 9 lid 1 Wwft.

Kortom: de instelling dient de cliënt te bevragen als dit nodig is gezien het risico en gezien de reeds bestaande informatiepositie van de instelling. Daarbij zal de instelling wel moeten kunnen onderbouwen en vastleggen waarom in een bepaald geval een lagere mate van intensiteit is toegepast.

**QA3.40: Vraag**
Wat moet een instelling doen als de EC de lijst van HRTC verandert?

**Antwoord**
De verscherpte onderzoeksmaatregelen gelden vanaf het moment dat een land aan de lijst wordt toegevoegd. Vanaf dat moment past de instelling de maatregelen conform art. 9 Wwft toe.

Als een land door de Europese Commissie van de lijst is verwijderd hoeven de verscherpte onderzoeksmaatregelen niet meer toegepast te worden.

**QA3.41: Vraag**
In hoeverre moet het hoger leidinggevend personeel elke transactie gerelateerd aan een HRTC apart goedkeuren?

**Antwoord**
Het gaat erom dat de zakelijke relatie niet wordt aangegaan zonder goedkeuring door het hoger leidinggevend personeel. Ook het besluit om de zakelijke relatie voort te zetten wordt niet genomen zonder goedkeuring door het hoger leidinggevend personeel.

Hierbij is goedkeuring van individuele transacties door hoger leidinggevend personeel niet nodig. Het relevante vereiste in de wet ziet op een zakelijke relatie, niet op een transactie. De goedkeuring door het hoger leidinggevend personeel dient dus gegeven te worden op het aangaan van de relatie, bijvoorbeeld als onderdeel van het CDD-proces bij het 'onboarden' van een klant die woonachtig is in of voornemens is zaken te doen met een HRTC. De transacties die vervolgens onderdeel zijn van deze zakelijke relatie vallen onder de voortdurende controle (transactiemonitoring). Goedkeuring voor het voortzetten van de zakelijke relatie wordt verlangd indien de cliënt zaken gaat doen met een HRTC of transacties gedaan worden van of naar een HRTC, terwijl dit niet binnen het verwachte transactieprofiel van de cliënt past.

### GP3.36: Good practice – Transacties met HRTC in het transactieprofiel

Bij onboarding vraagt de instelling naar potentiële transacties gerelateerd aan een HRTC. Als de cliënt aangeeft transacties te gaan doen gerelateerd aan een HRTC verzamelt de instelling aanvullende informatie over onder meer de achtergrond van deze transacties en gaat de instelling na of de transacties passend zijn met het oog op het profiel van de cliënt. De instelling maakt op basis hiervan een risicoanalyse. Het cliëntendossier wordt ter goedkeuring voorgelegd aan het hoger leidinggevend personeel.

### GP3.37: Good practice – Raamwerk voor goedkeuring hoger leidinggevend personeel

De instelling borgt de goedkeuring door het hoger leidinggevend personeel door middel van beleid (senior management approval framework) waarin duidelijk is vastgelegd:

a. Wat de parameters zijn waarbinnen goedkeuring wordt gegeven voor zakelijke relaties met cliënten uit HRTC. Gevallen die daarbuiten vallen worden alsnog op case-by-case basis door het hoger leidinggevend personeel expliciet goedgekeurd.
b. Degenen die het beleid uitvoeren hebben voldoende kennis en ervaring om deze beoordeling te kunnen maken.
c. De frequentie en de wijze van rapportage aan het hoger leidinggevend personeel.
d. De wijze waarop het hoger leidinggevend personeel 'goedkeuring' geeft binnen het raamwerk.
e. De controle door de compliancefunctie en de auditfunctie.

### GP3.38: Good practice – Voortdurende verscherpte controle

De instelling ziet bij het aangaan van de zakelijke relatie dat de cliënt transacties zal verrichten gerelateerd aan een HRTC. De zakelijke relatie wordt aangegaan na goedkeuring door het hoger leidinggevend personeel, volgens de regels die gelden binnen de instelling.

De transacties die vervolgens plaatsvinden binnen deze zakelijke relatie vallen onder de voortdurende verscherpte controle (transactiemonitoring). In gevallen waarbij transacties worden gedaan die buiten het verwachte transactieprofiel van de cliënt vallen, wordt bekeken of de relatie al dan niet kan worden voortgezet.

### GP3.39: Good practice – Toeristische uitgaven

Een cliënt is op vakantie in een HRTC en doet daar toeristische uitgaven. Uit hoofde van de verscherpte controle op transacties gerelateerd aan een HRTC merkt de instelling dit op. De instelling analyseert de transacties, betrekt daarbij de transactie-informatie als aanvullende informatie, en concludeert dat er sprake is van toeristische uitgaven, met een laag risico op witwassen en financieren van terrorisme.

## 3.7 Omgang met overige hogere risico's en verscherpt cliëntenonderzoek

Bepaalde typen cliënten of producten kunnen een inherent verhoogd integriteitsrisico meebrengen. Het is belangrijk dat instellingen bij hun risicoanalyse alert zijn op factoren die op een inherent verhoogd risico wijzen en extra maatregelen treffen om het integriteitsrisico te mitigeren. Deze risico-inschatting is cliëntspecifiek.

Tegelijkertijd is het ongewenst dat instellingen risico's onnodig te hoog inschatten. Dit zou er anders toe leiden dat beheersmaatregelen te veel en te intensief zijn, met als potentieel gevolg dat bonafide cliënten geconfronteerd worden met een hoge administratieve belasting of onnodig geweigerd worden. Dit onderstreept het belang van de risicogebaseerde benadering waarbij ook geldt: waar risico's lager zijn, volstaan eenvoudiger maatregelen.

### Q&A

**QA3.42: Vraag**

Wanneer moet een instelling verscherpt cliëntenonderzoek doen?

**Antwoord**

De Wwft onderscheidt een aantal situaties waarin verscherpt cliëntenonderzoek nodig is.[132] Verscherpt cliëntenonderzoek wordt onder andere toegepast in de volgende gevallen:

- Indien de zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of financieren van terrorisme met zich brengt.

132 Art. 8 lid 1 Wwft.

- Indien de cliënt woonachtig is, gevestigd is of zijn zetel heeft in een door de Europese Commissie op grond van artikel 9 van de vierde anti-witwasrichtlijn aangewezen staat met een hoger risico op witwassen of financieren van terrorisme (HRTC).
- Bij complexe of ongebruikelijk grote transacties en transacties met een ongebruikelijk patroon of zonder duidelijk economisch of rechtmatig doel.

**QA3.43: Vraag**
Welke factoren geven een indicatie van een potentieel hoog risico?

**Antwoord**
De instelling neemt in de risicobeoordeling in ieder geval de niet-limitatieve lijst van risicofactoren mee die genoemd is in bijlage III van de vierde anti-witwasrichtlijn.[133] Deze factoren geven een indicatie wanner er sprake is van een potentieel hoger risico.
Ook andere instanties reiken risicofactoren aan, bijvoorbeeld de EBA 'ML/TF Risk Factors Guidelines' en 'EBA report on ML/TF risks associated with payment institutions' van de European Banking Authority of de Guidance van de Financial Action Task Force (FATF).[134]

**QA3.44: Vraag**
In hoeverre zijn er sectoren die inherent hoge risico's met zich brengen?

**Antwoord**
Er zijn sectoren waarvan algemeen bekend is dat deze kwetsbaarder zijn voor integriteitsrisico's en die daarmee een hoger integriteitsrisicoprofiel hebben. Dit betekent echter niet dat aan alle cliënten in de betreffende sector per definitie een hoog risicoprofiel toegekend moet worden. Het betekent ook niet dat een cliënt die actief is in een 'laag risico sector' per definitie geen hoger integriteitsrisico kan meebrengen.

De sector waarin een cliënt actief is, is een van de factoren die de instelling meeweegt in de bepaling van de risicoclassificatie van de cliënt. Deze risicoclassificatie is cliëntspecifiek en derhalve niet generiek van toepassing op cliënten in de betreffende sector.

**QA3.45: Vraag**
Is cash altijd een hoog risico?

**Antwoord**
Nee. Contant geld is een wettig betaalmiddel, waarvan het legitieme gebruik niet gehinderd mag worden. In beginsel doet een instelling onderzoek als een transactie bijvoorbeeld niet past bij het profiel van de betreffende cliënt of als er hoog-risico-indicatoren naar boven komen. Het gebruik van contant geld kan een indicator zijn, maar moet altijd in samenhang met andere indicatoren worden beoordeeld.

Biljetten van EUR 500 verdienen bijzondere aandacht. Sinds januari 2019 geven nationale banken in de Eurozone geen biljetten van EUR 500 meer uit. Hoewel het biljet van EUR 500 een wettig betaalmiddel is, is er bij transacties met biljetten met relatief veel hoge coupures (EUR 500 en ook EUR 200) een verhoogd risico op criminele activiteiten.

133 Art. 8 lid 2 Wwft.
134 EBA (2021), Guidelines on ML/TF Risk Factors.

**QA3.46: Vraag**
Betekent de aanwezigheid van een factor die wijst op een hoog risico dat een cliënt daarmee als hoog risico geclassificeerd wordt?

**Antwoord**
Nee. Een instelling bepaalt zelf aan de hand van een risicobeoordeling of er sprake is van een hoog-risicosituatie waarbij verscherpt cliëntenonderzoek wordt toegepast. Instellingen houden in hun risicobeoordeling ten minste rekening met de risicofactoren zoals genoemd in bijlage III van de vierde anti-witwasrichtlijn. Deze factoren zijn handvatten om in te kunnen schatten of er sprake is van een hoog-risicosituatie. De lijst met risicofactoren is niet uitputtend, er kunnen ook andere factoren zijn die een indicatie zijn van hoog risico.

Instellingen stellen beleid en procedures op aan de hand van hun risicobeoordeling en identificeren in welke gevallen er sprake is van hoog risico. De aanwezigheid van een hoog-risicofactor impliceert niet automatisch dat de cliënt als hoog risico geclassificeerd moet worden. Alle relevante factoren spelen een rol bij het bepalen van het risicoprofiel.

**QA3.47: Vraag**
Als een cliënt een hoog risico heeft, moet de instelling hem dan afwijzen?

**Antwoord**
Nee, de beslissing om een zakelijke relatie met een specifieke cliënt aan te gaan is aan de instelling zelf en zal mede gebaseerd zijn op de risicobereidheid van de instelling en de mogelijkheid om geïdentificeerde integriteitsrisico's te kunnen beheersen.

**QA3.48: Vraag**
Kan een instelling op grond van de Wwft besluiten een hele sector of een groep cliënten met vergelijkbare kenmerken als onacceptabel te bestempelen?

**Antwoord**
Nee, de Wwft biedt geen grondslag om een hele sector of groep cliënten met vergelijkbare kenmerken categoraal als 'onacceptabel' te bestempelen.[135] Een instelling kijkt naar de cliëntspecifieke kenmerken bij het maken van een risico-inschatting. Hierbij kan het opereren in sectoren met een verhoogd risico op witwassen of terrorismefinanciering een cliëntkenmerk zijn, net als relaties met landen die worden gezien als een verhoogd risico op witwassen/terrorismefinanciering.

De instelling voorkomt onnodige weigering van cliënten of transacties door adequate cliëntspecifieke toepassing van maatregelen die gebaseerd zijn op een cliëntspecifieke risicobeoordeling.

**QA3.49: Vraag**
Wat houdt een verscherpt cliëntenonderzoek in?

**Antwoord**
In gevallen waarin volgens de instelling een hoger risico bestaat op witwassen of financieren van terrorisme, neemt de instelling aanvullende beheersmaatregelen (bovenop de reguliere maatregelen). Deze maatregelen verschillen per risico. De aanvullende maatregelen die de instelling treft zijn afhankelijk van de risicobeoordeling ten aanzien van de betreffende cliënt, transactie, product en het betrokken land of gebied. De intensiteit van het onderzoek is risicogebaseerd.

135 Een instelling kan bijvoorbeeld wel op eigen gronden overwegen dat ze zich in haar dienstverlening richt op bepaalde sectoren, en dat zij geen cliënten accepteert die niet in een van die sectoren actief zijn.

**QA3.50: Vraag**
Mag de instelling ook op afstand de cliënt identificeren en verifiëren?

**Antwoord**
Ja, dit mag. Wel wordt niet-fysieke aanwezigheid van de client op grond van bijlage III van de vierde anti-witwasrichtlijn gezien als risicofactor. Art. 8 Wwft verwijst naar deze bijlage.

Instellingen bepalen op basis van een risicogebaseerde benadering welke maatregelen worden genomen om het hogere risico van niet-fysieke aanwezigheid te compenseren. De maatregelen die worden genomen op grond van art. 8 Wwft komen bovenop de maatregelen die op grond van art. 3 Wwft moeten worden genomen. Dat cliënten op afstand geaccepteerd zijn door het toepassen van, bijvoorbeeld, innovatieve technieken betekent niet dat deze cliënten per definitie een hoge risicoclassificatie meekrijgen na acceptatie.

Bij niet-fysieke aanwezigheid zal de instelling meerdere onafhankelijke en betrouwbare bronnen raadplegen dan wel innovatieve technologieën toepassen om het risico te mitigeren. Hoe de instelling dit proces inricht bepaalt de instelling zelf met inachtneming van art. 3, 5 en 8 Wwft. Het is van belang dat de instelling dit proces vastlegt en regelmatig actualiseert.

## GP3.40: Good practice – Verzamelen aanvullende infomatie

Bij de acceptatie van cliënten die een product met een verhoogd risico afnemen, of producten (of combinaties daarvan) die afwijken van standaardproducten, volstaat de instelling niet met alleen standaardprocedures. Naast het controleren of de cliënt of andere betrokkenen voorkomen op de sanctielijsten, of men kredietwaardig is, of identiteitsdocumenten echt zijn en of de cliënt voorkomt in interne of externe waarschuwingssystemen van instellingen, verzamelt de instelling aanvullende informatie.

Welke aanvullende informatie verzameld wordt, baseert de instelling op het risicoprofiel van de cliënt (cliëntspecifiek). De instelling bekijkt per geval wat nodig is, waarbij aanvullende informatie betrekking kan hebben op het verkrijgen en beoordelen van informatie over de zakelijke activiteiten van de cliënt, de reputatie van de cliënt en van de UBO's, alsmede van personen waarmee deze geassocieerd worden. In het kader van het verscherpte cliëntenonderzoek doet de instelling in bepaalde gevallen onderzoek naar de bron van de middelen.

## GP3.41: Good practice – Hogere risico's en mitigerende maatregelen

Een instelling beschouwt een cliënt die is gevestigd in een HRTC of in een land met een significant corruptieniveau als hoog risico. Dit geldt ook als er sprake is van een cliënt met een UBO die is gevestigd in een dergelijk land.

Bij cliënten die geen natuurlijke persoon zijn, treft de instelling maatregelen om de juridische status van de cliënt vast te stellen. Voor transacties en zakelijke relaties die verband houden met deze gebieden voert de instelling extra controles uit op de zakelijke relatie, en bepaalt zij in welke

gevallen zij het uitvoeren van transacties beperkt qua aantal en omvang dan wel helemaal niet uitvoert. De instelling legt dit bij de cliëntacceptatie vast.

### GP3.42: Good practice – Risico's met betrekking tot de structuur en bedrijfsvoering

Een instelling heeft in het beleid vastgelegd in welke situatie er sprake is van een verhoogd risico met betrekking tot juridische entiteiten. Dit betreft ten minste:

- Entiteiten waar meer dan een door de instelling vastgesteld percentage van het geldverkeer in contanten plaatsvindt, rekening houdend met wat in de betreffende branche gebruikelijk is.
- Entiteiten met een structuur met meer dan twee lagen.
- Entiteiten die gevolmachtigde aandeelhouders hebben of aandelen aan toonder, omdat deze anonimiteit in de hand werken.

### GP3.43: Good practice – Omgang met cash-intensieve cliënten

Een instelling besteedt in haar beleid aandacht aan cliënten die relatief veel gebruik maken van contant geld. De instelling ziet contant geld als een factor die kan leiden tot een hoger risico, omdat de herkomst minder makkelijk te bepalen is. De instelling heeft in haar beleid vastgelegd dat bij cash-intensieve cliënten die, in samenhang met andere factoren, een hoog risico vormen, extra onderzoek wordt gedaan naar de herkomst van deze geldstromen.

De instelling heeft indicatoren vastgesteld op basis waarvan de diepgang van het onderzoek wordt bepaald (o.a. ten aanzien van het al dan niet bevragen van de cliënt) om de plausibiliteit van de bron van middelen vast te stellen, onder meer: de hoogte van het bedrag, de opgegeven reden van de herkomst van de middelen, land van herkomst of bestemming van de middelen, en geleverde product of dienst.

Tegelijkertijd voorkomt de instelling onnodige weigering van cliënten of transacties door cliëntspecifieke toepassing van maatregelen die gebaseerd zijn op een cliëntspecifieke risicobeoordeling.

## 3.8 Risicoprofiel

Het doel van de Wwft is het voorkomen van betrokkenheid bij witwassen en financieren van terrorisme. Daarbij is de Wwft risicogebaseerd: de intensiteit van de maatregelen ter voorkoming van witwassen en financieren van terrorisme dient te worden afgestemd op de concrete risico's die een cliënt meebrengt. Bij een verhoogd risico is meer aandacht nodig, bij een geringer risico kan worden volstaan met een minder intensieve controle.

Bij het identificeren en analyseren van de risico's hoort ook het indelen van cliënten in risicocategorieën op grond van het risico dat de cliënt met zich brengt. Door een risicoprofiel op te stellen kunnen instellingen tijdens de cliëntrelatie voortdurend bekijken of de relatie en de verrichte transacties nog overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel. Als bijvoorbeeld blijkt dat de verrichte transacties afwijken, dan stelt de instelling het risicoprofiel bij. Op die basis kan de instelling ook bepalen of minder dan wel meer maatregelen nodig zijn om de risico's te mitigeren.

## Q&A

**QA3.51: Vraag**
Moet altijd een risicoprofiel worden toegekend?

**Antwoord**
Ja, het uitgangspunt voor de beheersing is en blijft de risicoanalyse, en het risicoprofiel dat daaruit volgt. Bij het opstellen van een risicoprofiel van de cliënt worden de relevante risicofactoren in aanmerking genomen die tijdens het cliëntenonderzoek naar voren zijn gekomen. Uiteindelijk heeft een instelling inzicht in de ratio en passendheid van de transacties en producten voor die cliënt zodat signalen van witwassen en terrorisme financiering daarbij opvallen.

---

**QA3.52: Vraag**
Kan een instelling voor het vaststellen van het risicoprofiel van de cliënt gebruik maken van referentiegroepen ('peer groups')?

**Antwoord**
Ja. Een instelling kan het risicoprofiel van de cliënt mede bepalen aan de hand van bijvoorbeeld referentiegroepen. Daarbij definieert de instelling haar eigen referentiegroepen aan de hand van een aantal cliëntkenmerken, bijvoorbeeld: sectoren, rechtsvormen, leeftijd, inkomen, land, et cetera.
In de praktijk zal niet iedere cliënt passen in een vooraf gedefinieerde referentiegroep. Een dergelijke cliënt wordt apart geanalyseerd.

**QA3.53: Vraag**
Blijft een risicoprofiel van een cliënt altijd gelijk?

**Antwoord**
Nee. Het risicoprofiel kan in de loop der tijd wijzigen. Door middel van een review van de cliënt kan de instelling vaststellen of de cliënt nog steeds aan het vastgestelde risicoprofiel voldoet. De frequentie en diepgang van de review zijn afhankelijk van het risico dat de cliënt meebrengt.
De cliëntreview is onderdeel van de voortdurende controle van de cliënt.

**QA3.54: Vraag**
Hoe verhoudt het transactieprofiel zich tot het risicoprofiel?

**Antwoord**
Het transactieprofiel van de client draagt bij aan het vaststellen van het risicoprofiel. Het transactieprofiel stelt instellingen in staat om te controleren dat de transacties die tijdens de duur van de relatie worden verricht, overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel, en te bepalen of deze bijstelling behoeft.[136] Het is mogelijk dat het verwachte transactieprofiel van de cliënt aan de hand van referentiegroepen ('peer-grouping') wordt opgesteld.

Gedurende de duur van de relatie is het van belang dat de instelling doorlopend monitort of de cliënt aan het risicoprofiel voldoet en het transactiepatroon overeenkomstig de verwachtingen is. Dit is onderdeel van de voortdurende controle van de cliënt.

### GP3.44: Good practice – Referentiegroepen
Voor cliënten met een lager risico maakt een instelling gebruik van referentiegroepen om een transactieprofiel te bepalen. Deze cliënten worden niet van tevoren bevraagd op hun verwachte transacties. Als de feitelijke transacties afwijken van dit profiel dan gaat de instelling na of het profiel nog past bij de cliënt en of de cliënt anders ingedeeld zou moeten worden. Bij relatief veel afwijkingen gaat de instelling na of de referentiegroepen bijstelling behoeven.

### GP3.45: Good practice – Indelen van cliënten in risicocategorieën
De instelling maakt onderscheid in risicocategorieën (laag, normaal, hoog en onacceptabel) tussen haar klanten en neemt passende beheersmaatregelen.

## 3.9 Vastleggen van gegevens

Een instelling legt de documenten en gegevens met betrekking tot het cliëntenonderzoek op opvraagbare wijze vast.[137] Dit stelt de instelling in staat om het risicoprofiel te onderbouwen en om gedrags-/transactiepatronen tijdig te signaleren en te beoordelen. Tevens kunnen interne en externe toezichthouders de naleving van de Wwft door de instelling op basis van deze vastlegging beoordelen. Tot slot kan de instelling waar nodig gegevens verstrekken aan FIU-NL en aan opsporingsdiensten.

### Q&A

**QA3.55: Vraag**
Welke documenten en gegevens moeten worden vastgelegd?

**Antwoord**
Art. 33 Wwft specificeert welke documenten en gegevens de instelling ten minste vastlegt. Het is daarbij van belang dat uit het cliëntendossier het risicoprofiel blijkt en de onderbouwing daarvan. De gegevens die moeten worden vastgelegd zijn alle gegevens die zijn verkregen tijdens het cliëntenonderzoek, zoals kopieën van de identiteitsdocumenten, rekeninggegevens, correspondentie, gespreksnotities over en met de cliënt, transacties van en andere dienstverlening aan die cliënt. Artikel

136 Art. 3 lid 2 onder d. Wwft.
137 Art. 33 Wwft.

33 lid 2 Wwft bepaalt welke documenten en gegevens ten minste moeten worden vastgelegd. Uit het dossier blijkt ook hoe het besluitvormingsproces rond de cliëntacceptatie is verlopen.

In de Richtsnoeren 'Identificatie en verificatie van persoonsgegevens' van het College Bescherming Persoonsgegeven, de huidige Autoriteit Persoonsgegevens (AP), staat opgenomen dat een financiële instelling – als bewijs van de identificatieverplichting (reconstructieplicht) – ook een kopie van het gecontroleerde identiteitsdocument kan vastleggen.[138] Op grond van art. 33 Wwft bestaat er geen verplichting om het Burgerservicenummer (BSN) vast te leggen. Op de website van de AP is ook informatie te vinden over hetgeen banken wel en niet mogen bewaren.[139]

**QA3.56: Vraag**
Hoe lang moeten de documenten en gegevens bewaard blijven?

**Antwoord**
De documenten en gegevens worden gedurende vijf jaar na het tijdstip van het beëindigen van de zakelijke relatie of tot vijf jaar na het uitvoeren van de desbetreffende transactie bewaard.[140]

**QA3.57: Vraag**
Maakt het uit hoe de documenten en gegevens vast worden gelegd?

**Antwoord**
Ja. De instelling legt de documenten en gegevens op opvraagbare wijze vast.[141] De documenten en gegevens moeten toegankelijk zijn.[142]
De instelling beschikt over systemen die haar in staat stellen onverwijld en volledig te reageren op vragen van de FIU en van de toezichthoudende autoriteit.[143]

### GP3.46: Good practice – Vastlegging in cliëntendossier
Een instelling legt alle documenten en gegevens met betrekking tot het cliëntenonderzoek per cliënt vast in een overzichtelijk cliëntendossier. Het cliëntendossier is goed toegankelijk, onder andere voor analisten binnen de instelling die signalen vanuit transactiemonitoring analyseren en voor de compliance officer.

### GP3.47: Good practice – clientacceptatiecomité
Een instelling heeft een clientacceptatiecomité ingericht waarin het hoger leidinggevend personeel de meer complexe gevallen bespreekt en over acceptatie een besluit neemt.
De bespreking en het besluit worden consistent vastgelegd op een toegankelijke plek.
De opvolging van besluiten en eventueel aanvullende mitigerende maatregelen wordt bewaakt en vastgelegd door een daartoe aangewezen functionaris.

138 wetten.overheid.nl/BWBR0033181/2012-07-12.
139 autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/financiele-ondernemingen.
140 Art. 33 lid 3 Wwft.
141 Art. 33 lid 1 Wwft.
142 Art. 33 lid 3 Wwft.
143 Art. 33 lid 4 Wwft.

## 3.10 Binnen risicotolerantie?

Het kan voorkomen dat een cliënt buiten de risicotolerantie van de instelling valt met betrekking tot witwassen of financieren van terrorisme. In dat geval concludeert een instelling op basis van het cliëntenonderzoek en het vastgestelde risicoprofiel dat een bestaande of voorgenomen relatie met een cliënt te grote integriteitrisico's met zich brengt voor de instelling.

In bepaalde gevallen schrijft de Wwft dwingend voor wanneer een cliënt niet mag worden geaccepteerd dan wel wanneer een bestaande relatie moet worden beëindigd.[144]

### Q&A

**QA3.58: Vraag**
Op welke wijze vindt de afweging plaats of de cliënt binnen de risicotolerantie valt?

**Antwoord**
Een instelling legt in haar beleid vast welke risico's al dan niet acceptabel zijn, rekening houdend met de wettelijke vereisten omtrent bijvoorbeeld HRTC. De instelling beoordeelt vervolgens op individuele basis of een cliënt binnen de risicotolerantie valt. Dit is verbonden aan het risicoprofiel.
Een instelling kan vooraf bepalen dat bepaalde risicoprofielen - die bijvoorbeeld kunnen worden ingedeeld bij bepaalde referentiegroepen – geaccepteerd kunnen worden, al dan niet onder voorwaarden.

**QA3.59: Vraag**
Moet een instelling elk risico op betrokkenheid bij witwassen of financieren van terrorisme uitsluiten?

**Antwoord**
Nee. In hun rol als poortwachter weren instellingen criminele geldstromen uit het financiële systeem. Conform het gedachtegoed van de Wwft dient de instelling zich daarbij te baseren op een risico-inschatting. De instelling kan immers niet volledig uitsluiten dat een cliënt betrokken is bij witwassen of terrorismefinanciering. De beslissing om een zakelijke relatie aan te gaan is gebaseerd op een onderbouwde risico-inschatting en op de mogelijkheid om deze risico's te kunnen beheersen.

Van instellingen wordt daarmee verwacht dat zij alle redelijke maatregelen hebben getroffen om te voorkomen dat zij betrokken raken bij witwassen of financieren van terrorisme. De risicobenadering houdt ook in dat geaccepteerd wordt dat nooit volledig kan worden voorkomen dat, ondanks mitigerende maatregelen, toch criminele geldstromen door het financiële systeem gaan.
Van instellingen wordt niet verwacht dat zij dit volledig kunnen uitsluiten, er is dus een geaccepteerd 'restrisico'.

**QA3.60: Vraag**
Bepaalt DNB welke cliënten wel of niet aangenomen kunnen worden?

**Antwoord**
Nee, de instelling accepteert al dan niet de cliënt. De instelling baseert zich daarbij op de eisen die de Wwft stelt, haar beheersmaatregelen en haar eigen risicobereidheid

144 Zie art. 4 en 5 Wwft.

### GP3.48: Good practice – Beleid risicotolerantie

Een instelling heeft in haar beleid vastgelegd in welke gevallen volgens de wet cliënten niet mogen worden geaccepteerd en bestaande relaties moeten worden beëindigd, en in welke gevallen cliënten buiten haar eigen risicotolerantie vallen. Dit is in ieder geval als er sprake is van:

- Problemen bij het verifiëren van de identiteit van de cliënt of de UBO.
- Cliënten die anoniem wensen te blijven dan wel fictieve identiteitsgegevens verstrekken.
- Shell-banks (banken die geen fysieke aanwezigheid hebben in het land waar ze gevestigd zijn en een vergunning hebben).
- Cliënten die op een sanctielijst staan.
- Cliënten van wie blijkt dat, bijvoorbeeld mede op basis van aanvullende informatie, de combinatie van het type cliënt met de producten die deze wil afnemen onacceptabele risico's meebrengt.
- Cliënten die geen of onvoldoende informatie willen verstrekken over (dan wel ontoereikende documentatie ter verificatie daarvan kunnen overleggen) de aard en achtergrond van de cliënt, het doel van de zakelijke relatie, en in het bijzonder de bron van de middelen van de cliënt.
- Cliënten waarvan de organisatiestructuur van de cliënt of het doel van de structuur waar de doelvennootschap toe behoort na onderzoek onnodig complex of niet transparant blijken te zijn zonder dat hier een logische, bedrijfseconomische verklaring voor is.
- Professionele tegenpartijen die niet over de vereiste vergunningen beschikken.
- Cliënten die de dienstverlener onvoldoende inzicht in structuren, geldstromen en/of hun fiscale motieven geven.

### GP3.49: Good practice – Buiten risicotolerantie

Een potentiële cliënt wil een rekening openen bij een bank. De cliënt is een lokale bakkerij. Uit het cliëntenonderzoek blijkt dat de lokale bakkerij onderdeel is van een grotere structuur. De bakkerij is daarin de enige entiteit waarin economische activiteit plaatsvindt. De UBO is van de bakkerij is burger van een bekend Europees belastingparadijs, en stuurt de structuur aan vanuit een Zuid-Amerikaanse jurisdictie. De bank oordeelt dat de cliëntstructuur buiten de risicotolerantie valt.

## 3.11 Accepteren en toekennen niveau van beheersing

Als de cliënt binnen de risicotolerantie past, kan deze geaccepteerd worden. In het kader van de risicobeheersing past de instelling mitigerende maatregelen toe op de zakelijke relatie. Het niveau van beheersing moet passen bij het risicoprofiel van de cliënt: de intensiteit van de maatregelen ter voorkoming van witwassen en financieren van terrorisme dient te worden afgestemd op de concrete risico's die een cliënt meebrengt. Bij een verhoogd risico is meer aandacht nodig, bij een geringer risico kan worden volstaan met een minder intensieve controle. Dit is weer van belang voor de goede toegang tot de financiële infrastructuur en de proportionele belasting van zowel de cliënt als van de instelling.

### Q&A

**QA3.61: Vraag**
In hoeverre mag een instelling een cliënt accepteren voordat het cliëntenonderzoek is uitgevoerd?

**Antwoord**
Het cliëntenonderzoek vindt plaats vóórdat de instelling een zakelijke relatie aangaat of een incidentele transactie uitvoert.[145]

Er is een aantal uitzonderingen, o.a.:

- Een instelling mag de identiteit van de cliënt en de UBO verifiëren tijdens het aangaan van de zakelijke relatie, indien dit noodzakelijk is om de dienstverlening niet te verstoren en er weinig risico op witwassen of financieren van terrorisme bestaat. In dat geval verifieert de instelling de identiteit zo spoedig mogelijk na het eerste contact met de cliënt.[146]
- Verificatie van de identiteit van de begunstigde van een levensverzekering vindt plaats op het tijdstip van uitbetaling van de levensverzekering.[147]
- Een bank of andere financiële onderneming mag een rekening openen voordat de verificatie van de identiteit van de cliënt heeft plaatsgevonden, indien zij waarborgt dat deze rekening niet kan worden gebruikt voordat de verificatie heeft plaatsgevonden.[148] Dit geldt in deze lijn ook voor betaalinstellingen. Een betaalinstelling mag daarbij de gelden niet naar de merchant overmaken voordat de verificatie van de identiteit heeft plaatsgevonden, maar de betaalinstelling kan al wel collecteren.[149]

145 Art. 4 lid 1 en art. 5 lid 1 Wwft.
146 Art. 4 lid 3 Wwft.
147 Art. 3a lid 2 Wwft.
148 Art. 4 lid 4 Wwft.
149 Zie art. 4 lid 3 Wwft.

### GP3.50: Good practice – Aanvullende maatregelen

Een instelling past de volgende aanvullende maatregelen toe bij hogere risico's:

- Frequentere reviews op de zakelijke relatie.
- Bij transacties diepgaander onderzoek naar de rationale en naar de bron van de middelen.
- Verplichte advisering door de afdeling Compliance over het accepteren of voortzetten van de zakelijke relatie.
- 'Bad press' monitoring.

## 3.12 Weigeren cliënt

Het is van belang dat criminele geldstromen worden geweerd uit het financiële stelsel. Instellingen dienen daarom te voorkomen dat zij cliënten accepteren die een onacceptabel risico vormen.

### Q&A

**QA3.62: Vraag**
Wanneer mag een instelling een cliënt niet accepteren?

**Antwoord**
In onder meer de volgende gevallen accepteert een instelling een cliënt niet:

- indien er geen cliëntenonderzoek is verricht (behoudens de uitzonderingen genoemd in QA3.61);[150]
- indien het cliëntenonderzoek nog niet is uitgevoerd of afgerond;[151]
- indien het cliëntenonderzoek niet heeft geleid tot het beoogde resultaat;[152]
- indien de instelling niet beschikt over alle identificatie- en verificatiegegevens en overige gegevens inzake de identiteit van de cliënt, UBO en eventuele vertegenwoordigers;[153]
- indien een cliënt een onacceptabel risico vormt voor de instelling.

### GP3.51: Good practice – Cliëntacceptatiebeleid

Een instelling heeft in haar cliëntacceptatiebeleid en de werkinstructies duidelijk opgenomen onder welke omstandigheden de relatie met de cliënt wordt geweigerd.

## 3.13 Het melden bij de Financiële Inlichtingen Eenheid (FIU-NL)

Als een cliëntenonderzoek niet leidt tot het beoogde resultaat dan wel dat een zakelijke relatie wordt beëindigd, én indien de instelling daarbij aanwijzingen heeft dat de (potentiële) cliënt betrokken is bij witwassen of het financieren van terrorisme dan doet de instelling een melding bij de Financiële Inlichtingen Eenheid (FIU-NL).[154]

Naast de bovengenoemde gevallen meldt een instelling een verrichte of voorgenomen ongebruikelijke transactie onverwijld nadat het ongebruikelijke karakter van de transactie bekend is geworden – zie verder paragraaf 4.1.5.

150 Art. 5 lid 1 onder a Wwft
151 Behoudens enkele uitzonderingen, zoals die uit art. 4 Wwft.
152 Art. 5 lid 1 onder b Wwft.
153 Art. 5 lid 1 onder c Wwft.
154 Art. 16 lid 4 Wwft.

## GP3.52: Good practice – Melding en toelichting

Een instelling ontvangt van een onderneming een aanvraag voor een financiering, een zakelijke lening voor het financieren van verhuurd vastgoed. Uit het onderzoek blijk dat er sprake is van verschillende opmerkelijke zaken. De aanvrager laat in korte tijd een flinke groei van de vastgoedportefeuille zien. Verder wordt in een aantal gevallen de woningen door particulieren aan de onderneming verkocht onder de WOZ-waarde, terwijl zij op de reguliere woningmarkt een hogere prijs hadden kunnen ontvangen.

De instelling besluit deze voorgenomen transactie te melden aan de FIU. In de melding wordt uiteengezet wat voor financieringsproduct het betreft en welke overwegingen hebben geleid tot de conclusie dat de voorgenomen transactie ongebruikelijk is. De omstandigheden worden gedetailleerd uiteengezet in de transactieomschrijving en de betrokkenen bij de transactie zijn allen opgevoerd als partij in de meldingen.

## GP3.53: Good practice – Melding en toelichting

Een bank meldt een aantal ongebruikelijke transacties betreffende de aan- en verkoop van voertuigen. Uit de melding blijkt dat de instelling per tegenpartij een grondig open bronnenonderzoek heeft gedaan. De bank geeft deze informatie mee, waaruit o.a. blijkt dat partijen die autobedrijven lijken te zijn, geen online aanwezigheid hebben en gevestigd zijn in een woonhuis. Ook valt een aantal tegenpartijen op omdat er een relatie lijkt te zijn met een groot fraudeonderzoek, waaraan in de melding wordt gerefereerd. Daarnaast maakt de toelichting duidelijk dat er auto's worden ingekocht door branchevreemde partijen, en ontvangt de onderneming huur- en borgbetalingen voor vrachtwagens, terwijl dat geen bedrijfsactiviteit van de onderneming is.

In de transactieomschrijving worden niet alleen transacties opgesomd, maar is puntsgewijs uiteengezet waarom de gemelde transacties ongebruikelijk zijn. Er zijn meerdere transacties gemeld, deze worden in de melding aan elkaar verbonden.

Als bijlage voegt de instelling een volledig rekeningoverzicht van de relevante periode bij de melding, die context en inzicht geeft in het rekeningverloop van de cliënt. Hierdoor kan de FIU-onderzoeker gelijk een onderzoek starten.

# 4 Cliëntenonderzoek: voortdurende controle

## 4.1 Transactiemonitoring

Instellingen zijn verplicht een voortdurende controle uit te oefenen op de zakelijke relatie en de tijdens de duur van deze zakelijke relatie verrichte transacties.[155] Het doel hiervan is:

- om te verzekeren dat de transacties overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel[156]
- om criminele geldstromen te weren
- om ongebruikelijke transacties te (kunnen) detecteren en te melden[157]
- om ervoor te zorgen dat de gegevens met betrekking tot de cliënt actueel gehouden worden.[158]

Financieel-economische criminaliteit ondermijnt onze maatschappij. Financiële instellingen spelen als poortwachter een belangrijke rol bij het voorkomen hiervan. Een instelling die adequaat de transacties monitort die in het kader van haar dienstverlening worden uitgevoerd, kan tijdig actie ondernemen als sprake is van een situatie waarbij er aanleiding is om te veronderstellen dat de transactie verband kan houden met witwassen of financieren van terrorisme, of van een transactiepatroon dat daarop wijst.

- De instelling kan die transacties nader onderzoeken en indien nodig melden bij FIU-NL. FIU-NL kan de transactie verder analyseren en waar nodig als verdacht doormelden aan de opsporingsinstanties.
- Ook kan de instelling vermoedelijke witwas- of terrorismefinancieringstransacties detecteren en weigeren.

Een gebrekkige monitoring maakt de instelling kwetsbaar waardoor zij (onbewust) bijdraagt aan het financieren van terrorisme of het (schuld)witwassen van geld.

Transactiemonitoring is daarmee een essentiële maatregel om potentieel criminele geldstromen te detecteren. Instellingen besteden daarbij bijzondere aandacht aan ongebruikelijke transactiepatronen en transacties van cliënten, die naar hun aard een hoger risico op witwassen of het financieren van terrorisme met zich brengen.[159] Is er aanleiding om te veronderstellen dat een (voorgenomen) transactie verband houdt met witwassen of terrorismefinanciering, dan moet een instelling deze transactie als ongebruikelijk melden bij de FIU-NL.[160]

155 Art. 3 lid 2 onder d. Wwft.
156 Art. 3 lid 2 onder d Wwft.
157 Art. 16 lid 1 Wwft.
158 Art. 3 lid 11 Wwft. Art. 14 lid 4 Bpr.
159 Art. 2a lid 1 Wwft.
160 Art. 16 lid 1 Wwft.

## Q&A

**QA4.1: Vraag**
Wat is een transactie?

**Antwoord**
Onder transactie wordt verstaan: handeling of samenstel van handelingen van of ten behoeve van een cliënt waarvan de instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen.[161] Deze definitie omvat meer dan alleen bijvoorbeeld betalingstransacties.

Met de definitie van transactie is beoogd duidelijk te maken dat een ongebruikelijke transactie van de cliënt, of van een derde ten behoeve van de cliënt, altijd moet worden gemeld indien een instelling daarvan heeft kennisgenomen ten behoeve van haar dienstverlening aan die cliënt. Een direct of causaal verband tussen de ongebruikelijke transactie en de werkzaamheden van de instelling is geen vereiste. De woorden "handeling of samenstel van handelingen van of ten behoeve van een cliënt" dienen zo te worden uitgelegd dat ook een passieve betrokkenheid van de instelling (doordat zij wetenschap heeft van de transactie) de wettelijke meldplicht kan activeren.[162]

**QA4.2: Vraag**
Wat is een ongebruikelijke transactie?

**Antwoord**
Een ongebruikelijke transactie in de zin van de Wwft is een transactie die op grond van de indicatoren bedoeld in art. 15 lid 1 Wwft als ongebruikelijk is aan te merken. Deze indicatoren zijn opgenomen in de bijlage van artikel 4 Uitvoeringsbesluit Wwft 2018.

De indicatoren zijn onderverdeeld in objectieve indicatoren en de subjectieve indicator.

- Objectieve indicatoren beschrijven een situatie waarin een transactie altijd onverwijld moet worden gemeld.
- De subjectieve indicator verplicht een instelling om een transactie te melden indien er aanleiding is om te veronderstellen dat de transactie verband kan houden met witwassen of financieren van terrorisme. Dit vraagt van de instelling een beoordeling of een transactie ongebruikelijk is.

Bij indicatoren die zijn gerelateerd aan een grensbedrag beoordeelt de instelling ook of er sprake is van een verband tussen twee of meerdere transacties. Dit kan aan de hand van het soort transactie en de bedragen waar het om gaat. Indien er een verband is en de transacties gezamenlijk het grensbedrag overschrijden, meldt de instelling deze transacties onder de subjectieve indicator – ook als niet helemaal zeker is dat de transacties samen één geheel vormen, maar er wel gegronde vermoedens zijn.

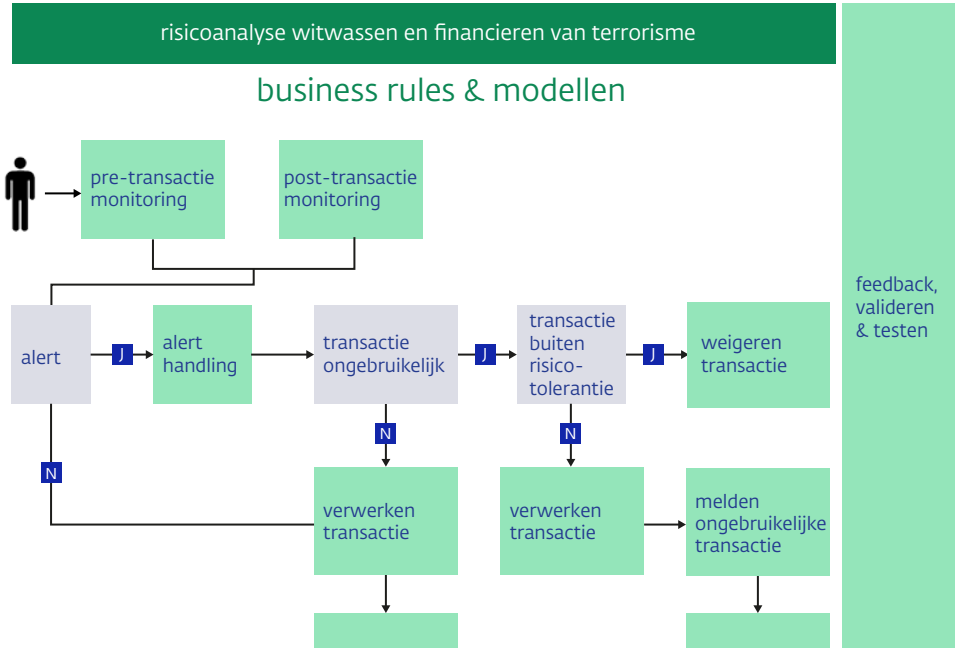
161 Art. 1 lid 1 Wwft.
162 Kamerstukken II 2011-2012, 33 238, nr. 3, p. 10. In de wetsgeschiedenis komt een aantal voorbeelden van deze situatie aan de orde. Zo kan een accountant een ongebruikelijke transactie opmerken in de administratie van de cliënt. Een ander voorbeeld is een notaris die ten behoeve van een zogenoemde ABC-levering kennisneemt van een ongebruikelijk prijsverschil tussen de AB- en de BC-transactie. In lijn hiermee kan een bank bijvoorbeeld een ongebruikelijke waarde opmerken in een handelstransactie.

**QA4.3: Vraag**

Moet transactiemonitoring altijd geautomatiseerd plaatsvinden?

**Antwoord**

Nee. Instellingen richten het transactiemonitoringsproces risicogebaseerd in. De inrichting hangt onder meer af van de aard en omvang van de instelling, van de risico's waar de instelling mee




geconfronteerd wordt en van het aantal transacties dat door de instelling wordt uitgevoerd.

Er is geen verplichting tot geautomatiseerde transactiemonitoring. Als sprake is van grotere aantallen transacties, dan ligt het in de rede om de transactiemonitoring geautomatiseerd te laten plaatsvinden om de effectiviteit, consistentie en doorlooptijd van monitoring te kunnen borgen. Het gaat erom dat de instelling ongebruikelijke transacties en potentieel criminele geldstromen effectief detecteert.

**QA4.4: Vraag**

De inrichting van transactiemonitoring is een dynamisch proces; wat betekent dat?

**Antwoord**

In hoofdstuk 2 wordt besproken dat de risicoanalyse het uitgangspunt is voor de inrichting van de beheersing, inclusief transactiemonitoring. De risicoanalyse brengt de relevante en belangrijkste risico's met betrekking tot witwassen en financieren van terrorisme in kaart. Op basis hiervan bepaalt de instelling hoe de transactiemonitoring moet worden ingericht om de risico's aantoonbaar te beheersen.

Omdat risico's veranderen, is dit een dynamisch proces:

- Op basis van de aard en omvang van het risico (bijv. cash, betalingen naar hoog risicolanden) bepaalt de instelling welke business rules en modellen (met bijbehorende drempelwaarden) het risico kunnen detecteren.
- Aan de hand van (historische) transactiedatasets test de instelling of de risico's voldoende worden gedetecteerd met de gekozen business rules, modellen en grenswaarden, waarna wordt overgegaan tot implementatie in de bedrijfsvoering.
- Na de implementatie van een passende set aan maatregelen, monitort de instelling of de output van het transactiemonitoringsysteem aansluit bij de geïdentificeerde risico's en legt de overwegingen daarbij vast.
- De vaststelling dat een risico nog onvoldoende wordt gedetecteerd kan leiden tot aanvullende mitigerende maatregelen door de instelling.

## Elementen transactiemonitoring

Hierna wordt een aantal elementen met betrekking tot transactiemonitoring toegelicht.
Het uitgangspunt hiervoor is onderstaand schema, waarin het proces van transactiemonitoring op hoofdlijnen is weergegeven. Dit schema is bedoeld om de bespreking van transactiemonitoring te structureren en betreft niet een door de Wwft voorgeschreven gang van zaken.

Het stroomschema kan worden beschouwd als een hulpmiddel bij het lezen van dit hoofdstuk en als een manier om de verschillende onderdelen van de transactiemonitoring in kaart te brengen. Het bovenste element, de risicoanalyse witwassen en financieren van terrorisme, is in paragraaf 2.1 al besproken. De risicoanalyse is het uitgangspunt is voor het opstellen van beleid en procedures met betrekking tot transactiemonitoring. Dit leidt tot de business rules & modellen. Deze business rules & modellen zijn de handvatten aan de hand waarvan de transactiemonitoring wordt uitgevoerd. Met behulp van validatieonderzoek en feedback-loops verscherpt een instelling de business rules & modellen waar nodig.

In de paragrafen hierna komen de volgende elementen aan de orde:
- Business rules & modellen
- Pre-transactiemonitoring
- Post-transactiemonitoring
- Alert handling
- Melden van ongebruikelijke transacties
- Feedback en testen.

### 4.1.1 Business rules & modellen

De risicoanalyse ligt aan de basis van de maatregelen om witwassen en het financieren van terrorisme tegen te gaan. Dat geldt ook voor transactiemonitoring. De kennis die de instelling toepast om ongebruikelijke of verdachte transacties te kunnen detecteren, is toegesneden op de risico's die de instelling loopt.[163] Zo zullen de gebruikte business rules passend moeten zijn voor de detectie (en mitigatie) van de risico's zoals benoemd in de risicoanalyse en de scenario's uit die analyse.

De kennis die de instelling toepast om ongebruikelijke of verdachte transacties te kunnen herkennen dan wel detecteren is daarmee meer dan algemene kennis van bijvoorbeeld typologieën. Het gaat om kennis over hoe de instelling betrokken kan raken bij witwassen of financieren van terrorisme, gegeven het bedrijf en de bedrijfsvoering.

#### Q&A

**QA4.5: Vraag**
Is het voldoende als een instelling standaardmodellen toepast voor het detecteren van ongebruikelijke transacties?

**Antwoord**
Nee. Standaardmodellen kunnen een startpunt zijn, maar een instelling kan hier niet enkel op vertrouwen. Een transactiemonitoringsysteem dient te passen bij het risicoprofiel van de instelling, en gevoed te worden door toegepaste kennis (intelligence) vanuit de instelling. De business rules van het transactiemonitoringsyteem dienen passend te zijn om de risico's die de instelling loopt effectief te mitigeren. De instelling legt het verband tussen de risicoanalyse en het transactiemonitoringssysteem vast.

---

**QA4.6: Vraag**
In hoeverre is het opstellen van een transactieprofiel op basis van de verwachte transacties verplicht?

**Antwoord**
De instelling stelt het risicoprofiel van de cliënt vast.[164] Een transactieprofiel op basis van de verwachte transacties of het verwachte gebruik van de rekening van een cliënt (expected transaction profile,

163 Vgl. art. 2a-2c Wwft. Daarbij besteedt een instelling bijzondere aandacht aan ongebruikelijke transactiepatronen en aan transacties die naar hun aard een hoger risico op witwassen of financieren van terrorisme met zich brengen.
164 Art. 3 lid 2 onder d Wwft.

ETP) kan in verband daarmee een goed hulpmiddel zijn om ongebruikelijke transacties te detecteren. Door het verwachte transactiegedrag van de cliënt in beeld te brengen kunnen instellingen toetsen of de door de cliënt uitgevoerde transacties afwijken.

Het ETP moet in dat kader wel worden gezien als een middel, en is geen doel op zich. Ongebruikelijke transacties kunnen ook op andere manieren gedetecteerd worden, bijvoorbeeld door middel van de toepassing van scenario's of van geavanceerde modellen.

**QA4.7: Vraag**
In hoeverre kan er gebruik worden gemaakt van referentiegroepen?

**Antwoord**
Het is niet altijd mogelijk om voor iedere individuele relatie op voorhand een individueel (maatwerk) risicoprofiel op te stellen, gelet op de omvangrijke aantallen relaties voor bepaalde cliëntsegmenten, bijvoorbeeld bancaire dienstverlening aan particulieren of klein MKB. Om dit praktisch te kunnen doen, kan een instelling haar zakelijke relaties indelen naar bijvoorbeeld referentiegroepen (peer groups), en het individuele risicoprofiel hierop baseren. Daarbij definieert de instelling haar referentiegroepen aan de hand van een aantal cliëntkenmerken, bijvoorbeeld sectoren, rechtsvormen, leeftijden, natuurlijke personen, transactiegedrag, inkomen, landen, et cetera.

Een ETP kan ook voor een referentiegroep worden opgesteld. Wel is het van belang dat de referentiegroepen voldoende homogeen zijn qua cliëntgedrag, zodat het ETP voldoende nauwkeurig kan worden bepaald.

**QA4.8: Vraag**
Is er een model dat voor alle instellingen toepasbaar is?

**Antwoord**
Nee. De business rules en de modellen zijn toegespitst op de risico's die van toepassing zijn op de instelling. Dat betekent dat een instelling zelf analyseert welke business rules en modellen voor haar relevant zijn. Het is derhalve belangrijk om de inrichting van het transactiemonitoringsysteem te koppelen aan de uitkomsten en inzichten uit de risicoanalyse. Daarmee maakt de instelling inzichtelijk welke risico's het grootst zijn binnen de cliëntenportefeuille van de instelling en op welke wijze het transactiemonitoringsysteem bijdraagt aan detectie en mitigatie van de risico's.

Omdat een instelling zich ontwikkelt en risico's wijzigen, heeft de instelling een proces ingericht om de effectiviteit van de gebruikte business rules en modellen systematisch te monitoren en te beoordelen – en waar nodig bij te stellen. Het is altijd van belang dat de instelling in staat is om ongebruikelijke transactiepatronen en transacties die naar hun aard een hoger risico op witwassen of financieren van terrorisme met zich brengen, te detecteren.[165]

165 Art. 2a lid 1 Wwft.

## GP4.1: Good practice – Intelligence en transactiemonitoring

*Intelligence* (toegepaste kennis over cliënten en typologieën) kan bijdragen aan effectieve transactiemonitoring:

- Instellingen die een beperkt aantal transacties verwerken kunnen mogelijk volstaan met handmatige monitoring van transacties. Ook in die gevallen wordt dit proces gevoed met toegepaste kennis om ongebruikelijke of verdachte transacties te kunnen detecteren. Deze kennis is dan bijvoorbeeld neergelegd in een handboek of in werkinstructies.
- Instellingen waarbinnen transactiemonitoring geautomatiseerd plaatsvindt, maken in de regel gebruik van instructies en detectieregels om potentiële witwas- en terrorismefinancieringspatronen te detecteren, bijvoorbeeld in de vorm van scenario's en bijbehorende grensbedragen (business rules).
- Instellingen maken hiervoor ook gebruik van modellen en/of van kunstmatige intelligentie (artificial intelligence, AI) en/of machine learning. Een voorbeeld hiervan zijn de modellen die klanten met outliergedrag (t.o.v. hun referentiegroep) detecteren. Ook kan worden gedacht aan modellen die netwerkanalyses maken, of modellen die op basis van historische FIU-meldingen transacties met vergelijkbare kenmerken kunnen destilleren uit transactiedata.

## GP4.2: Good practice – Koppeling met risicoanalyse

Een verzekeraar heeft ten behoeve van haar transactiemonitoring een set aan business rules opgesteld. In deze business rules heeft de verzekeraar de in de SIRA geïdentificeerde risico's en scenario's verwerkt. Een van de SIRA-scenario's die is omgezet in een business rule betreft de detectie van transacties met betrekking tot vervroegde afkoop boven een bepaald grensbedrag. Op deze transacties verricht de instelling standaard een plausibiliteitscheck, voor zover deze in een eerder stadium nog niet in voldoende mate is verricht. Deze plausibiliteitscheck houdt onder meer in dat de instelling nagaat of de ingelegde premies verklaarbaar zijn.

## GP4.3: Good practice – Opzet business rules

Een instelling heeft de opzet, inrichting en adequaatheid van business rules goed onderbouwd. Hierbij heeft de instelling onder meer aandacht besteed aan:

a. duidelijke vaststelling van grenswaarden
b. differentiatie in de business rules tussen grenswaarden voor hoog risico cliënten in het kader van verscherpte monitoring
c. differentiatie in de business rules tussen grenswaarden voor verschillende business segmenten (Small and Medium Enterprises (MKB), Corporate, Financial Institutions).

## GP4.4: Good practice – Koppeling business rules en risicoanalyse

Een bank heeft de in het transactiemonitoringsysteem opgenomen business rules opgesteld op basis van de risicoanalyse (SIRA). Het verband tussen de SIRA en de business rules heeft de bank vastgelegd.

Bij het opstellen van de business rules houdt de bank rekening met verschillende factoren:

- het soort cliënt (particulier en zakelijk)
- het cliëntsegment, bijvoorbeeld onderscheid tussen private banking of retail; waarbinnen andere gesegmenteerde doelgroepen zijn te onderscheiden, zoals professionele sportbeoefenaars;
- het cliëntrisicoprofiel, zoals opgesteld bij cliëntacceptatie en waar nodig later aangepast;
- het land waar de transactie naartoe gaat of vandaan komt;
- het product, bijvoorbeeld sparen, vastgoedfinanciering of handelsfinanciering;
- de distributiekanalen, bijvoorbeeld fysieke aanwezigheid van de klant of online;
- de aard en frequentie van de transacties, bijvoorbeeld giraal of contant;
- het risicoprofiel van de cliënt, bijvoorbeeld laag, midden of hoog;
- internationale transacties die vanuit offshore landen via Nederland doorgeboekt worden naar andere offshore landen.

Verder wordt bij het bepalen van de business rules ook gebruik gemaakt van vergelijkingen met andere transacties van de cliënt en met de referentiegroep. Bij de business rules wordt niet alleen rekening gehouden met de genoemde factoren, maar worden de gestelde drempelwaarden ook goed en waar mogelijk datagedreven onderbouwd.

De door de instelling in de transactiemonitoring gedetecteerd risico's betrekt zij in de evaluatie van haar SIRA.

### GP4.5: Good practice – Business rules terrorismefinanciering

Een instelling beschikt voor het detecteren van terrorismefinanciering over een lijst met red flags en mogelijke business rules die kunnen duiden op terrorismefinanciering. Voor deze lijst en voor het bijhouden daarvan maakt de instelling gebruik van waarschuwingslijsten en gepubliceerde cases en typologieën.

### GP4.6: Good practice – Ongebruikelijke transacties via outlier detectie

Op basis van data-analyse en modellen detecteert een instelling outliers. Hierbij wordt onder meer gekeken naar transactievolumes, aantallen transacties, transacties naar hoog-risicolanden of -sectoren, en ook naar afwijkende patronen in gebruikte IP-adressen of andere technische kenmerken. Hierdoor detecteert de instelling ook ongebruikelijke transacties die niet met behulp van de business rules worden geïdentificeerd. De instelling gebruikt de resultaten hiervan voor het aanscherpen van haar risk appetite.

### GP4.7: Good practice – Risk appetite en business rules

In haar risicoanalyse heeft een instelling ook haar risk appetite vastgelegd. Daarbij heeft ze vastgesteld welke activiteiten (in termen van aard en omvang) buiten haar risk appetite vallen. Een instelling gebruikt haar risk appetite vervolgens door deze te vertalen naar business rules. Op basis hiervan heeft de instelling in haar business rules onder meer passende grenswaarden gedefinieerd voor het aantal tikkies, cryptobetalingen, betalingen van en naar hoog risicolanden, cash opnames en stortingen. Dit betekent dat transacties die boven deze grenswaarden komen door het transactiemonitoringsysteem worden opgemerkt, waarna ze nader onderzocht worden.

### GP4.8: Good practice – Contant geld

In de set met business rules heeft een bank regels opgenomen met betrekking tot het gebruik van contant geld. Deze regels zijn gebaseerd op de risicoanalyse. De bank heeft daarbij een risk appetite geformuleerd. Hierin is opgenomen dat bij midden- en kleinbedrijven contante transacties onder een bepaalde grenswaarde geen alert genereren. Bij het bepalen van deze grenswaarde wordt rekening gehouden met de aard van het bedrijf.

Op basis hiervan wordt uitzonderlijk hoog cash-gebruik en het veelvuldig gebruik van grote coupures dat niet past bij het bedrijfsmodel van de cliënt opgemerkt. Voor een cliënt die een individuele transactie onder een door de bank bepaalde grenswaarde doet, wordt – bijkomende bijzonderheden daargelaten – geen alert gegenereerd.

## GP4.9: Good practice – Hoog-risicojurisdicties

Een instelling heeft in haar transactiemonitoringsysteem extra aandacht voor hoog-risicojurisdicties. Om te bepalen wat hoog-risicojurisdicties zijn, hanteert de instelling meerdere bronnen:

- De lijst van hoog-risicolanden van de Europese Commissie.
- De waarschuwingslijsten van de FATF.
- De Corruption Perceptions Index van Transparency International.
- Een interne lijst die wordt bijgehouden op basis van eigen analyses, incidenten, FIU-meldingen en (internationale) witwasschandalen.

### 4.1.2 Pre-transactiemonitoring, vermoedelijke ML/TF-transactie

Een instelling mag in ieder geval geen transacties uitvoeren die witwassen en/of financieren van terrorisme faciliteren, of waar het vermoeden bestaat dat dit het geval is. Ook bij overige transacties moeten instellingen een afweging maken of deze gelet op de risico's op witwassen en/of financieren van terrorisme kunnen worden uitgevoerd. Het is van belang dat instellingen adequate maatregelen treffen om ongebruikelijke transacties te detecteren, ook voordat deze uitgevoerd worden.

Pre-transactiemonitoring vindt plaats voordat de transactie is uitgevoerd. Door middel van pre-transactiemonitoring kunnen ongebruikelijke transacties, of (andere) transacties die buiten de risicotolerantie van de instelling vallen, mogelijk al vóór het uitvoeren of tijdens de uitvoering van de transacties gedetecteerd worden. Een vermoedelijke ML/TF-transactie valt per definitie buiten de risicotolerantie en wordt niet uitgevoerd.

### Q&A

**QA4.9: Vraag**

Wanneer is er sprake van een vermoedelijke ML/TF-transactie?

**Antwoord**

Bij een vermoedelijke ML/TF-transactie is er sprake van de aanmerkelijke kans op het faciliteren van witwassen of financieren van terrorisme. De omstandigheden van het geval bepalen of hier sprake van is. Naast vermoedelijke ML/TF-transacties kunnen er ook andere (ongebruikelijke) transacties zijn die buiten de risicotolerantie van de instelling vallen. Dit kan bijvoorbeeld het geval zijn als de instelling aanleiding heeft om te veronderstellen dat er sprake kan zijn van witwassen of financieren van terrorisme, en uit nader onderzoek naar de transactie en de herkomst van de middelen er twijfels blijven. Een instelling heeft verscherpte aandacht voor complexe of ongebruikelijk grote transacties, voor transacties met een ongebruikelijk patroon of zonder duidelijk economisch of rechtmatig doel. Deze transacties worden nader onderzocht.[166]

**QA4.10: Vraag**

Hoe moet pre-transactiemonitoring worden ingericht?

**Antwoord**

Pre-transactiemonitoring kan zowel geautomatiseerd als handmatig plaatsvinden. Het proces stelt de instelling in staat om ongebruikelijke transacties al voor uitvoering te detecteren en waar nodig te stoppen.

166 Art. 8 lid 3 Wwft.

## GP4.10: Good practice – Business rules

Een instelling heeft specifieke richtlijnen opgesteld op basis waarvan medewerkers bij een voorgenomen transactie kunnen bepalen of er sprake is van een ongebruikelijke transactie. Transacties die hieraan voldoen, worden doorgeleid naar de compliance officer en, na definitieve beoordeling op ongebruikelijkheid, eventueel gemeld – en waar nodig geweigerd.

## GP4.11: Good practice – Oplopende geldtransacties, weigeren dienstverlening

Een geldtransactiekantoor ziet dat een cliënt geregeld geld overmaakt naar de Filipijnen voor 'family support'. Het totaalbedrag loopt in 2 maanden op naar meer dan EUR 10.000. Na een kort onderzoek concludeert het kantoor dat er geen plausibele reden is voor de omvang van de transacties. De reeds uitgevoerde transacties worden gemeld aan de FIU.

De volgende dag wil de cliënt EUR 3.000 storten. Uit navraag blijkt dat de cliënt geen plausibele reden geeft voor de omvang van de stortingen. De cliënt kan ook niet duidelijk maken hoe hij aan het geld komt. De instelling heeft een sterk vermoeden van witwassen en weigert de transactie. De instelling doet ook aangifte bij de politie en meldt de voorgenomen transactie aan de FIU.

## GP4.12: Good practice – Weigeren afkoop polis verzekeraar

Een cliënt sluit een polis af bij een verzekeraar. Via de tussenpersoon stort de cliënt EUR 750.000 op de polis. Vier maanden later wil de cliënt de polis beëindigen, waarbij hij een afkoopsom van de verzekeraar ontvangt.
De verzekeraar concludeert dat er een aanmerkelijke kans bestaat op het faciliteren van witwassen, en weigert de afkoop. De storting en de voorgenomen afkoop worden gemeld aan de FIU. De verzekeraar doet ook aangifte bij de politie.

## GP4.13: Good practice – Vermoedelijke witwastransactie

Een bank is betrokken bij de verkoop van vastgoed van een cliënt die in faillissement is.
De opbrengsten van de verkoop van het object komen toe aan de bank. Er meldt zich een geïnteresseerde partij uit een jurisdictie die een reputatie heeft als veilige haven voor criminele gelden. De bank vraagt door en desgevraagd geeft de geïnteresseerde partij aan dat de financiering komt van een partij uit het Midden-Oosten die zijn vermogen heeft verworven met oliewinning in Zuid-Amerika. Als bewijs van de gelden verstrekt de partij een bankafschrift van een Aziatische vennootschap van de partij uit het Midden-Oosten.

Uit onderzoek van de bank blijkt dat de genoemde Zuid-Amerikaanse olievelden nauwelijks productief zijn. Uit verder onderzoek blijkt dat de Aziatische bank het verstrekte bankafschrift niet herkent.

De bank weigert de transactie, doet aangifte bij de politie en meldt de voorgenomen transactie aan de FIU.

## GP4.14: Good practice – Onderliggende producten handelsfinanciering komen niet overeen met cliëntprofiel

Een bank signaleert bij een aanvraag voor een documentair krediet dat de betrokken producten afwijken van de reguliere business van de cliënt. De transactie wordt 'on hold' gezet en bij de compliance officer gemeld. De compliance officer adviseert om navraag te doen bij de cliënt. Uit navraag door de accountmanager bij de cliënt blijkt dat de cliënt een tweede activiteit is begonnen en daarvoor investeringen doet. Het bewijs hiervan wordt inderdaad aangeleverd. Na akkoord van de compliance officer wordt de transactie alsnog uitgevoerd. De accountmanager werkt het cliëntendossier bij.

### 4.1.3 Post-transactiemonitoring & detectie ongebruikelijke transacties

Door middel van post-event transactiemonitoring kan de instelling transacties en transactiepatronen identificeren die wijzen op mogelijke betrokkenheid bij witwassen of financieren van terrorisme. De toegepaste kennis, bijvoorbeeld in de vorm van business rules en modellen, is cruciaal voor het genereren van de juiste alerts/signalen.

## Q&A

**QA4.11: Vraag**

Is het verplicht dat post-event transactiemonitoring geautomatiseerd wordt uitgevoerd?

**Antwoord**

Nee. De inrichting van het post-event transactiemonitoringsproces hangt sterk af van de aard en omvang van de instelling, en van het aantal transacties dat dagelijks door de instelling wordt uitgevoerd. De instelling maakt op basis van de risico's een keuze voor handmatig of geautomatiseerd monitoren, of voor een combinatie daarvan. Als er sprake is van grotere aantallen transacties, dan ligt het in de rede om de transactiemonitoring geautomatiseerd te laten plaatsvinden om de effectiviteit, consistentie en doorlooptijd van de monitoring te kunnen borgen.

---

**QA4.12: Vraag**

Wat is een alert?

**Antwoord**

Een alert is een signaal dat duidt op een mogelijk ongebruikelijke transactie. Dit zijn bijvoorbeeld transacties die buiten het verwachte patroon en/of profiel vallen of die geen economisch of juridisch doel hebben.

Alerts worden onder andere gegenereerd door het transactiemonitoringsysteem. De instelling volgt de alert op, zie hierna het gedeelte over alert handling (4.1.4).

**QA4.13: Vraag**
Welke transacties moeten instellingen monitoren?

**Antwoord**
In het kader van de Wwft monitort de instelling transacties die gerelateerd zijn aan de dienstverlening van de instelling. Een betaling van de instelling zelf aan een eigen leverancier valt hier bijvoorbeeld buiten. De instelling borgt dat alle bronsystemen van te monitoren transacties zijn geïdentificeerd en dat de data volledig en juist worden meegenomen in het transactiemonitoringproces. Dit kan data betreffen over de cliënt, de diensten en de transacties.

## GP4.15: Good practice – Verschillende methoden van alert generatie

Een instelling past een combinatie van detectiemethoden toe.

- Een deel van de monitoring vindt plaats met gebruikmaking van business rules. Hiermee kunnen onder andere transacties die voldoen aan de objectieve indicator worden geïdentificeerd. Ook kunnen afwijkingen van het verwachte transactieprofiel worden geconstateerd en nader onderzocht. Verder kan de instelling hiermee nagaan of typologieën die gezien haar risicoprofiel relevant zijn zich voordoen in haar transacties.
- Een deel van de monitoring vindt plaats met behulp van AI en modellen. Op deze manier kan de instelling mogelijk ongebruikelijke patronen en complexe transacties beter detecteren en nader onderzoeken.

## GP4.16: Good practice – Alert generatie bij combinatie van transacties

In korte tijd worden relatief kleine bedragen bij de instelling gestort. De bedragen hebben dezelfde bestemming. De bedragen vallen onder de grens van de objectieve indicator, maar opgeteld blijken deze bedragen er boven te komen.

Het transactiemonitoringsysteem genereert een alert. De instelling onderzoekt de alert en concludeert dat men waarschijnlijk bewust onder de meldgrens blijft. De instelling kwalificeert de transacties als ongebruikelijk (subjectieve indicator) en meldt deze aan de FIU.

## GP4.17: Good practice – Alert generatie terrorismefinanciering

Een instelling wordt geconfronteerd met een door een cliënt uitgevoerde pintransactie in een grensgebied aan een oorlogsland. Dit land wordt ook in verband gebracht met terrorisme. De instelling volgt de nieuwsberichten van FIU-NL nauwlettend, waaronder een lijst met plaatsnamen in het grensgebied. Het monitoringssysteem genereert op basis daarvan voor deze transactie een zogenaamd terrorismefinancieringsalert.

## GP4.18: Good practice – Transactiepatronen

Met behulp van het transactiemonitoringsysteem detecteert een instelling transactiepatronen of netwerken en combinaties van transacties – dat is een samenstel van transacties van een of meerdere cliënten die op geaggregeerd niveau kunnen duiden op witwassen of terrorismefinanciering. Door dit gebruik van voorspellende data-analyse (*predictive analytics*) kan de instelling geautomatiseerd en standaard bredere transactiepatronen, -structuren en netwerken van transacties detecteren.

### GP4.19: Good practice – Borging kwaliteit en volledigheid data

Een instelling borgt de kwaliteit en de volledigheid van de data die worden gebruikt bij het transactiemonitoringsysteem door het toepassen van (technische) functiescheiding (o.a. tussen test-, acceptatie-, en productieomgeving) en door controles op de volledigheid van de data.

De instelling heeft vooraf bepaald welke transacties en bijbehorende data moeten worden gecontroleerd. De instelling maakt hierbij gebruik van *Data Trace Analysis* om te borgen dat systemen en data tot op attribuutniveau zijn geïdentificeerd. Op basis hiervan heeft de instelling controlemaatregelen vastgesteld bij de bronsystemen en bij het transactiemonitoringsysteem. Deze maatregelen hebben betrekking op de kwaliteit (inhoudelijk) van de data en op de kwantiteit (volledigheid).

### 4.1.4 Alert handling

Alerts zijn signalen die wijzen op een mogelijk ongebruikelijke transactie. De instelling onderzoekt bij (een combinatie van) alerts of er daadwerkelijk sprake is van een ongebruikelijke transactie.

De behandeling van alerts (alert handling) met de daarbij behorende beoordeling van alerts is belangrijk:

- Elk signaal dient te worden behandeld. Een instelling mag niet het risico lopen dat ongebruikelijke transacties onopgemerkt blijven, en dat dergelijke transacties niet worden gemeld aan de FIU.
- Signalen kunnen niet zonder meer worden gemeld als ongebruikelijke transactie, in dat geval worden transacties onterecht als ongebruikelijk gemeld dan wel onterecht geweigerd.
- De beoordeling van een alert kan leiden tot een herbeoordeling van het risicoprofiel van de cliënt.

## Q&A

**QA4.14: Vraag**
In hoeverre moeten alerts worden gemeld?

**Antwoord**
Een alert is een signaal. De instelling onderzoekt bij (een combinatie van) alerts of er sprake is van een ongebruikelijke transactie en betrekt daarbij onder meer cliënt- en transactie-informatie. Waar nodig worden externe bronnen geraadpleegd en/of wordt de cliënt gevraagd naar de achtergrond en het doel van de transactie.
Het onderzoek naar de alerts en de bevindingen worden vastgelegd. De instelling gaat tot melding aan de FIU over indien de instelling concludeert dat er sprake is van een ongebruikelijke transactie.

---

**QA4.15: Vraag**
Waar moet alert handling aan voldoen?

**Antwoord**
Een instelling beschikt over procedures en werkprocessen om alerts te beoordelen en af te handelen. De betrokken medewerkers beschikken over actuele instructies en opleiding om ongebruikelijke transacties en vermoedelijke ML/TF-transacties te herkennen.[167]
De procedures en werkprocessen borgen dat de doorlooptijden vanaf het genereren van de alert tot aan de melding aan de FIU-NL beperkt blijven en dat de juiste prioriteiten in de afhandeling van de alerts kunnen worden gesteld.

Voorts is van belang dat de instelling vastlegt wat de overwegingen en conclusies zijn om een alert te sluiten en om de transactie al dan niet als ongebruikelijk te melden aan de FIU-NL.

---

**QA4.16: Vraag**
Wanneer is een transactie ongebruikelijk?

**Antwoord**
Indien een transactie aan bepaalde indicatoren voldoet, dan kwalificeert deze als ongebruikelijk.[168]
Voor verschillende categorieën instellingen zijn indicatoren vastgesteld.[169]

- De objectieve indicatoren beschrijven een situatie waarin een transactie altijd moet worden gemeld.
- De subjectieve indicator ziet op transacties waarbij de instelling aanleiding heeft om te veronderstellen dat deze verband kan houden met witwassen of financieren van terrorisme.

De subjectieve indicator vraagt om een eigen beoordeling door de instelling. Dit past in de risicogebaseerde benadering. Bij indicatoren die zijn gerelateerd aan een grensbedrag beoordeelt de instelling ook of er sprake is van een verband tussen twee of meerdere transacties. Dit kan aan de hand van het soort transactie en de bedragen waar het om gaat. Indien er een verband is, zouden deze transacties onder de subjectieve indicator als ongebruikelijk kunnen worden gekwalificeerd.

167 Art. 35 Wwft.
168 Art. 15 lid 1 Wwft.
169 Art. 4 jo. bijlage 1 Uitvoeringsbesluit Wwft 2018.

**QA4.17: Vraag**
Welke opvolging is van belang als een medewerker concludeert dat er sprake is van een ongebruikelijke transactie?

**Antwoord**
De organisatie is zodanig ingericht dat de eerste lijn een duidelijke verantwoordelijkheid heeft voor de transactiemonitoring en dat, voor zover de instelling hierover beschikt, de compliancefunctie een adviserende en controlerende taak heeft. Daarbij heeft de compliancefunctie ook een taak bij het melden van ongebruikelijke transacties aan de FIU-NL.[170] Het is daarmee van belang dat de instelling een procedure in werking heeft die erin voorziet dat de compliancefunctie betrokken wordt als er sprake is van een ongebruikelijke transactie.

---

**QA4.18: Vraag**
In hoeverre kan een alert automatisch gesloten worden?

**Antwoord**
Een instelling kan bepaalde alerts op grond van het risico geautomatiseerd sluiten. De volgende aandachtspunten zijn ten minste van belang:

- De instelling heeft een expliciete overweging ten aanzien van haar risk appetite met betrekking tot bepaalde transacties.
- De instelling heeft het onderliggende risicogebaseerde beslismodel goed gedocumenteerd.
- Een relatief groot aantal geautomatiseerd gesloten alerts kan wijzen op een niet adequaat beslismodel.
- De instelling heeft een procedure waarin de geautomatiseerd gesloten alerts geëvalueerd worden, bijvoorbeeld met het oog op transactiepatronen.

## GP4.20: Good practice – Vastlegging
In het kader van de alert handling documenteert de instelling of de betreffende transactie past in het transactiegedrag van de cliënt, en ook of de transactie logisch en plausibel is voor het soort cliënt en de sector waarin de cliënt actief is.

## GP4.21: Good practice – Training
Een instelling heeft zowel voor de eerste, tweede als derde lijn een (jaarlijks) trainingsprogramma beschikbaar. Naast het bespreken van ontwikkelingen op het gebied van wet- en regelgeving ligt de nadruk op casuïstiek uit de praktijk. Dit betreft praktijkvoorbeelden rondom mogelijk witwassen en financieren van terrorisme en hoe de instelling hiermee omgaat.

In de trainingen wordt zodoende de vertaling gemaakt van de praktijk en wet- en regelgeving naar beleid, procedures en onderliggende werkprocessen. Ook worden de medewerkers getraind in het gebruik van de verschillende (nieuwe) bronnen die voor de analyse beschikbaar zijn.
De instelling verschaft op die manier duidelijkheid aan medewerkers over hoe in voorkomende gevallen gehandeld dient te worden.

## GP4.22: Good practice – Capaciteit en middelen voor analyse
Een instelling geeft de analisten voldoende tijd voor een gedegen onderzoek en vastlegging van hun onderzoek. Zij hebben daarbij de beschikking over voldoende middelen, en toegang tot interne en externe systemen en informatiebronnen.

170 Art. 2d lid 3 Wwft.

Onderdeel daarvan is dat de analisten bij de beoordeling van alerts het cliëntendossier moeten kunnen raadplegen. Informatie in het cliëntendossier kan aanvullende informatie geven om een transactie met een verhoogd risico op witwassen en terrorismefinanciering te detecteren. Met informatie uit het cliëntendossier kan de analist bijvoorbeeld beoordelen of de transacties passen bij de activiteiten van een cliënt. Een andere informatiebron geeft inzicht in de gebruikte coupures voor opnames of stortingen.

De instelling gebruikt managementinformatie over de ontwikkeling in het aantal geopende en afgehandelde alerts met het oog op de benodigde capaciteit en middelen.

## GP4.23: Good practice – Analyse alert

Bij een instelling wordt door het transactiemonitoringsysteem een alert gegenereerd naar aanleiding van substantiële contante stortingen op een zakelijke rekening. In respons op deze alert wordt in de eerste plaats een brede analyse gemaakt van het cliënt- en transactieprofiel. Hierbij wordt vastgesteld dat de gebruikte rekening op naam staat van een horecagelegenheid, en dat in het CDD-dossier geen bijzondere risico's zijn onderkend. Uit een additioneel onderzoek naar de achtergrond van de cliënt blijken een transparante situatie en geen bijzonderheden uit het verleden.

Uit het transactieonderzoek blijkt dat contante stortingen op deze rekening geregeld voorkomen, waarbij het volume maandelijks fluctueert tussen de 5.000 en 15.000 euro. In de zomerperiode is dit volume eenmalig toegenomen tot meer dan 20.000 euro. In die specifieke periode is het in het risicoprofiel van de cliënt vastgestelde verwachte volume aan contante stortingen overschreden. In het onderzoek wordt vastgesteld dat de contante stortingen een stabiel percentage van de totale inkomsten vormen.

Op basis van de werkinstructie kan de alert-behandelaar, na onderzoek, bevestigen dat dit percentage conform de verhoudingen in deze sector zijn en ook gebruikelijk voor deze cliënt. Ook in de zomerperiode blijft de verhouding tussen cash en girale inkomsten beneden de door de instelling bepaalde grenswaarde. Dit is te verklaren binnen de reguliere bedrijfsactiviteiten van de cliënt, waarbij een seizoenspatroon en extra inkomsten in de zomerperiode gebruikelijk zijn.

Daarnaast wordt vastgesteld dat de uitgaande transacties vooral betrekking hebben op het doen van betalingen aan salaris, inkoop bij horecagroothandels, belastingen en huur. Ook deze uitgaande betalingen passen binnen gebruikelijke activiteiten van een horecaonderneming.

De alert-behandelaar concludeert op basis van de verrichte analyse dat de contante stortingen niet ongebruikelijk zijn. Er vindt geen melding plaats.

## GP4.24: Good practice – Analyse alert terrorismefinanciering

Twee maanden na een pintransactie in Oost-Turkije vraagt een cliënt een lening aan van EUR 10.000 bij de bank. De medewerker van de bank stelt vast dat vier maanden eerder aan deze cliënt reeds een lening is verstrekt van EUR 10.000, waarbij de cliënt had aangegeven dat de lening bedoeld was voor onder andere de aankoop van een auto.

De medewerker besluit nader onderzoek te doen en stelt vast dat het geld van de eerste lening vrijwel direct van de rekening is gehaald en in verschillende transacties naar Turkije is gestuurd. Ook vermoedt de medewerker een verband met de eerdere alert, de pintransactie in Turkije.

Naar aanleiding hiervan stelt de medewerker diverse vragen aan de cliënt, maar die kan geen duidelijke reden geven voor de transacties. De tweede lening wordt hierop geweigerd en na het verzoek voor de tweede lening worden alle transacties, zowel de pin-transactie als de beide

aangevraagde leningen, als ongebruikelijk aangemerkt. De volgende elementen/combinatie van red flags spelen daarbij een rol:

- een pintransactie in het grensgebied Turkije-Syrië
- afsluiten van een lening die in een zeer kort tijdsbestek geheel wordt opgenomen
- besteding van de lening correspondeert niet met de verklaring van de cliënt
- opknippen van gelden in kleinere bedragen voor overboekingen
- gelden verkregen via een lening overboeken naar bepaalde landen.

### 4.1.5 Melden ongebruikelijke transactie

Door ongebruikelijke transacties te melden aan de FIU-NL zijn de autoriteiten beter in staat gerichte opsporingsmiddelen in te zetten om witwassen en financieren van terrorisme tegen te gaan.

#### Q&A

**QA4.19: Vraag**

Wanneer moet een instelling melden?

**Antwoord**

Een instelling meldt een verrichte of voorgenomen ongebruikelijke transactie onverwijld nadat het ongebruikelijke karakter van de transactie bekend is geworden aan de FIU.[171]

**QA4.20: Vraag**

In hoeverre moet een transactie die in verband met witwassen of terrorismefinanciering aan de politie of het Openbaar Ministerie (OM) is gemeld, ook als ongebruikelijke transactie aan de FIU worden gemeld?

**Antwoord**

Het ligt in de rede dat transacties die in verband met witwassen of financieren van terrorisme aan politie of OM worden gemeld, ook aan de FIU worden gemeld; er is immers de veronderstelling dat deze transacties verband kunnen houden met witwassen of financieren van terrorisme.[172]

---

**QA4.21: Vraag**

In hoeverre heeft het doen van een melding aan de FIU strafrechtelijke en civielrechtelijke gevolgen voor de instelling?

**Antwoord**

Het belang van de meldplicht wordt onderstreept door de strafrechtelijke vrijwaring van art. 19 Wwft en de civielrechtelijke vrijwaring van art. 20 Wwft:

- De strafrechtelijke vrijwaring ziet erop toe dat gegevens of inlichtingen die de instelling te goeder trouw bij melding verstrekt, niet kunnen worden gebruikt ten behoeve van een opsporingsonderzoek of strafrechtelijke vervolging van de instelling ter zake van witwassen of financieren van terrorisme. De wet breidt deze vrijwaring uit tot degene die de melding heeft gedaan – bijvoorbeeld een medewerker die voor de melding heeft gezorgd of die aan het opstellen van het meldingsbericht heeft meegewerkt. Als een instelling op juiste wijze, in lijn met de vereisten van de Wwft, gegevens heeft vertrekt aan de FIU, kan deze instelling bijvoorbeeld niet strafrechtelijk worden vervolgd voor het delen van deze informatie met de FIU.

171 Art. 16 lid 1 Wwft. Art. 16 lid 4 Wwft geeft ook situaties aan waarvoor een meldplicht geldt, zie paragraaf 3.13.
172 Bijlage 1 Uitvoeringsbesluit Wwft 2018.

- De civielrechtelijke vrijwaring houdt in dat een instelling niet civielrechtelijk aansprakelijk is voor de schade die iemand anders (de cliënt of een derde) als gevolg van een melding lijdt wanneer is gehandeld in de redelijke veronderstelling dat uitvoering wordt gegeven aan de meldplicht. Hierbij kan gedacht worden aan eisen gesteld in een civielrechtelijke procedure op grond van wanprestatie, indien de instelling heeft besloten een transactie niet uit te voeren en deze te melden. Ook kan gedacht worden aan een actie op grond van een onrechtmatige daad, wegens eventuele schade die zou zijn ontstaan ten gevolge van een melding door een instelling.

Deze vrijwaringen gelden indien de melding te goeder trouw en op correcte wijze, conform de vereisten van de Wwft, heeft plaatsgevonden.

**QA4.22: Vraag**
Welke gegevens moeten worden gemeld aan de FIU?

**Antwoord**
De Wwft bepaalt welke gegevens bij een melding aan de FIU moeten worden verstrekt.[173]
De FIU kan met deze gegevens een ongebruikelijke transactie nader analyseren. Indien een instelling stelselmatig bepaalde gegevens niet aanlevert, kan de FIU deze omissie in het meldgedrag aan de toezichthouder doorgeven.[174] De toezichthouder kan hierop de instelling aanspreken, onder andere door een formele maatregel op te leggen.

De FIU kan n.a.v. een melding nadere gegevens of inlichtingen opvragen. Die moeten onverwijld worden verstrekt.[175]

**QA4.23: Vraag**
Wie doet de melding van ongebruikelijke transacties?

**Antwoord**
Van belang is dat ongebruikelijke transacties daadwerkelijk gemeld worden. Instellingen die niet beschikken over een compliancefunctie, kunnen zelf inregelen wie of welke afdeling verantwoordelijk is voor het melden van ongebruikelijke transacties. Indien de instelling beschikt over een compliancefunctie, dan bepaalt de Wwft dat deze verantwoordelijk is voor het melden van ongebruikelijke transacties. Dat betekent dat de compliancefunctie moet beschikken over de capaciteit, de bevoegdheden en de middelen om deze verantwoordelijkheid te kunnen nemen.[176] Hierdoor is geborgd dat het melden van ongebruikelijke transacties is gebaseerd op een onafhankelijk oordeel.

Bij de inrichting van het meldproces gelden de volgende uitgangspunten:
- De beslissing om tot melden over te gaan wordt op zelfstandige basis genomen. Dat betekent ook dat andere (eerstelijns) prioriteiten het meldproces niet mogen belemmeren c.q. beïnvloeden. De compliancefunctie (indien de instelling hierover beschikt) heeft de doorslaggevende stem.
- Degene die verantwoordelijk is voor de uitvoering van het meldproces heeft hiervoor voldoende bevoegdheden, capaciteit en middelen.
- Indien de uitvoering van het meldproces (gedeeltelijk) in de eerste lijn is belegd, wordt over het melden verantwoording afgelegd aan de compliancefunctie (indien de instelling hierover beschikt). De betrokken medewerkers moeten dit deel van hun werkzaamheden zelfstandig en onafhankelijk van de eerste lijn, kunnen uitvoeren.

173 Art. 16 lid 2 Wwft. Art. 16 lid 5 Wwft: indien het gaat om een melding op grond van art. 16 lid 4 Wwft, verstrekt de instelling ook een beschrijving van de redenen waarom art. 16 lid 4 Wwft van toepassing is.
174 Art. 13 onder g Wwft.
175 Art. 17 Wwft.
176 Art. 2d lid 3 Wwft.

**QA4.24: Vraag**

Wat moet een instelling doen met de gegevens over een ongebruikelijke transactie?

**Antwoord**

Een instelling bewaart de gegevens met betrekking tot de ongebruikelijke transactie. Dit betreft:[177]

- De gegevens die de instelling op grond van art. 16 lid 2 Wwft heeft gemeld aan de FIU en die noodzakelijk zijn om de desbetreffende transactie te kunnen reconstrueren.
- Een afschrift van de melding aan de FIU, inclusief de daarbij verstrekte informatie en gegevens.
- Het bericht van ontvangst van de melding dat door de FIU is gestuurd.

**QA4.25: Vraag**

Hoe lang moet een instelling de gegevens bewaren?

**Antwoord**

De bewaartermijn is 5 jaar na het tijdstip van het doen van de melding, respectievelijk het tijdstip van ontvangst van het bericht van de FIU. De gegevens zijn gedurende die periode goed toegankelijk.[178]

**QA4.26: Vraag**

Mag een instelling de cliënt inlichten over een melding?

**Antwoord**

Nee. Instellingen, en de personen die voor hen werkzaam zijn, zijn onder meer verplicht geheim te houden dat een melding van een ongebruikelijke transactie is gedaan.[179] Ook aan een cliënt op wie de melding betrekking heeft mag geen mededeling worden gedaan hierover (het zogenaamde *tipping off* verbod), omdat dit mogelijk de opsporing kan belemmeren.

**QA4.27: Vraag**

Zijn er uitzonderingen op de geheimhoudingsplicht?

**Antwoord**

Ja. Uitzonderingen op de geheimhoudingsplicht volgen uit de wet.[180]
De uitzonderingen staan bepaalde instellingen onder meer toe om informatie over een melding uit te wisselen met instellingen die behoren tot dezelfde groep en, onder strikte voorwaarden, met een andere instelling behorende tot dezelfde categorie. In het laatste geval dient de informatiedeling betrekking te hebben op een cliënt van beide instellingen en een transactie waarbij beide instellingen betrokken zijn, dient er sprake te zijn van gelijkwaardige geheimhoudingsplichten en gegevensbescherming, en dient de informatiedeling uitsluitend gericht te zijn op het voorkomen van witwassen en financieren van terrorisme

177 Art. 34 lid 1 Wwft.
178 Art. 34 lid 2 Wwft.
179 Art. 23 lid 1-4 Wwft.
180 Art. 23 lid 5, 6 Wwft.

Zonder deze uitzonderingen zouden waarschuwingssystemen tussen instellingen kunnen worden belemmerd. De uitwisseling van informatie moet passen binnen het doel van de wet en voldoen aan de wettelijke vereisten.

**QA4.28: Vraag**
In hoeverre mag een melding van een ongebruikelijke transactie binnen de groep gedeeld worden?

**Antwoord**
Een instelling deelt een melding binnen de groep, tenzij door de FIU anders wordt bepaald.[181]

---

**QA4.29: Vraag**
In hoeverre moet een instelling ook aangifte doen bij de politie?

**Antwoord**
Naast een melding aan FIU-NL is het mogelijk dat de instelling bij een sterk vermoeden van witwassen of financieren van terrorisme ook aangifte doet bij de politie.

---

**QA4.30: Vraag**
Moeten instellingen blijven melden bij de FIU indien er sprake is van een vordering van het OM?

**Antwoord**
Ja. Instellingen kunnen geconfronteerd worden met een vordering van het OM om cliëntinformatie te verstrekken in het kader van een strafrechtelijk onderzoek naar een cliënt (of naar derden).
De instelling kan informatie m.b.t. de vordering niet delen met haar cliënten. De verplichting tot het melden van ongebruikelijke transacties blijft gelden.

**QA4.31: Vraag**
Wat wordt er met een melding aan de FIU gedaan?

**Antwoord**
FIU-NL onderzoekt gemelde transacties.[182] Dit onderzoek kan ertoe leiden dat een transactie 'verdacht' wordt verklaard. In dat geval meldt de FIU de transactie aan de opsporingsinstanties. De instelling krijgt hier over het algemeen bericht van.

### GP4.25: Good practice – Procedure inzake meldingen

Een instelling meldt ongebruikelijke voorgenomen en uitgevoerde transacties onverwijld en volledig aan de FIU-NL. Hiervoor beschikt de instelling over een procedure hoe het meldproces er intern uitziet en waaruit blijkt hoe in voorkomende gevallen gehandeld dient te worden.
De procedure borgt ook dat er onverwijld wordt gemeld zodra het ongebruikelijke karakter van een transactie bekend is geworden.

Onderdeel van de procedure is dat eerdere en aanverwante transacties van de cliënt in het onderzoek worden betrokken om te beoordelen of er achteraf gezien sprake kan zijn van ongebruikelijke transacties die ook of alsnog gemeld moeten worden. Daarbij worden het risicoprofiel van de cliënt en het bijbehorende transactieprofiel heroverwogen.

181 Art. 23a Wwft.
182 Ik heb een melding gedaan, wat nu? (fiu-nederland.nl)

### GP4.26: Good practice – Training

Een instelling geeft voldoende guidance aan haar medewerkers over het melden van ongebruikelijke transacties door ieder kwartaal voorbeelden te bespreken en door deze ook op te nemen in het reguliere opleidingsprogramma.

### GP4.27: Good practice – Melden op basis van objectieve indicator

Met betrekking tot transacties die voldoen aan een objectieve indicator heeft een instelling een geautomatiseerd meldproces ingericht. De compliancefunctie toetst periodiek de werking hiervan.

Hiermee voorkomt de instelling dat ongebruikelijke transacties mogelijk niet onverwijld gemeld worden en vermindert ze de administratieve lasten.

### GP4.28: Good practice – Melden van transacties waarvan aangifte is gedaan

Een instelling meldt transacties die in verband met witwassen of terrorismefinanciering aan politie of het Openbaar Ministerie zijn gemeld, ook als ongebruikelijke transactie aan de FIU. Er is immers aanleiding om te veronderstellen dat de transactie verband kan houden met witwassen of terrorismefinanciering.

### GP4.29: Good practice – Geheimhouding

Een instelling heeft in beleid en procedures vastgelegd op welke wijze geheimhouding is geborgd. Dit omvat ook het toekennen van de juiste toegangsrechten van kernsystemen die worden gebruikt voor het afhandelen van alert meldingen van ongebruikelijke transacties en beveiliging van informatiestromen.

Dit omvat ook het periodiek verstrekken van guidance en training aan betrokken medewerkers, met name ook medewerkers die contact hebben met cliënten. Voor deze medewerkers is het essentieel om te weten wanneer mogelijk sprake is van ongebruikelijke transacties, welke vragen dan aan een cliënt gesteld moeten worden en welke informatie onder geen beding aan de cliënt mag worden gegeven.

#### 4.1.6 Feedback en testen

Een transactiemonitoringsysteem met de daarin toegepaste kennis dient te passen bij het risicoprofiel van de instelling (zie ook paragraaf 4.1.1). Dit betekent ook dat de gebruikte intelligence dynamisch is: risico's kunnen veranderen, en daarmee bijvoorbeeld ook de gebruikte business rules. Om risico's en ongebruikelijke transacties te kunnen blijven herkennen is het van belang dat het systeem en de toegepaste kennis actueel zijn. Nieuwe risico's en risico's die niet meer relevant zijn, leiden tot een ander risicoprofiel, waardoor bijstelling van het transactiemonitoringsysteem nodig kan zijn.

Verder kan er sprake van zijn dat bepaalde business rules en modellen niet effectief (meer) zijn: ze genereren te weinig true positives, te veel false negatives of te veel false positives. Om dit vast te kunnen stellen, is testen van het transactiemonitoringsysteem van belang – en daaropvolgend een eventuele bijstelling van het transactiemonitoringsysteem.

## Q&A

**QA4.32: Vraag**
Is evaluatie van transactiemonitoring nodig?

**Antwoord**
Ja. Een effectief transactiemonitoringsysteem is een essentieel element in de beheersing van het risico op betrokkenheid bij witwassen of financieren van terrorisme.

In dit verband is het passend dat de instelling het systeem van transactiemonitoring evalueert om te beoordelen of gebruikte business rules en modellen effectief zijn of mogelijk ineffectief. Dat kan bijvoorbeeld wanneer de business rules te grofmazig zijn, te hoge grenswaarden hebben of niet passen bij de instelling, waardoor nauwelijks sprake is van alerts op een bepaalde business rule. Een (periodieke) beoordeling is dan van belang om na te gaan of bepaalde business rules en modellen ten onrechte geen alerts hebben gegenereerd en of bijstelling mogelijk noodzakelijk is.

---

**QA4.33: Vraag**
Is testen ook bij geavanceerde technieken van belang?

**Antwoord**
Ja. Juist bij geavanceerde technieken is validatie van belang om onverwachte en mogelijk ongewenste uitkomsten tijdig te signaleren. Backtesten en vergelijking met andere detectietechnieken kunnen daarin een belangrijke rol spelen.

Bij zelflerende systemen is het daarbij van belang te borgen dat ontwikkelingen in het model niet geleidelijk tot niet-plausibele of ongewenste resultaten leiden. Dit kan bijvoorbeeld door te kijken of een model ook op een vooraf vastgestelde referentieset goed blijft functioneren.

**QA4.34: Vraag**
Wat is backtesting?

**Antwoord**
Evaluatie van business rules en modellen kan plaatsvinden door middel van het zogenoemde ‘backtesting’. Op basis van de uitkomsten van de backtest voert de instelling eventueel aanpassingen door in het transactiemonitoringsysteem.

Het doel van deze tests is de business rules en modellen verder te optimaliseren en effectiever te maken, zodat deze meer true positive alerts en minder false positive alerts kunnen generen.

Backtesting kan op verschillende manieren, zoals:

1. Een test waarbij achteraf een selectie van transacties wordt geanalyseerd die binnen de toenmalige configuratie van het systeem niet tot een alert hebben geleid. Het doel hiervan is vast te stellen of deze transacties terecht niet tot een alert hebben geleid (‘true negatives’) of dat bepaalde transacties toch indicatief zijn voor mogelijke ongebruikelijk gedrag (‘false negatives’).
2. Een analyse van de transacties die als mogelijk ongebruikelijk zijn opgemerkt via een andere route dan post-transactiemonitoring. Het doel van deze vorm van backtesting is te analyseren in hoeverre het transactiemonitoringsysteem in staat is deze ongebruikelijke transactiepatronen en transacties te detecteren.
3. Een test waarbij business rules met veel of alleen maar ‘false positive’ alerts worden geanalyseerd. Het doel van deze test is te onderzoeken of deze business rules wel relevant zijn en eventueel hoe deze business rules, na aanpassing, verhoudingsgewijs meer ‘true positives’ kunnen genereren.
4. Een test waarbij achteraf de tijdigheid van meldingen van ongebruikelijke transacties wordt geanalyseerd met het doel om die te verbeteren.

## GP4.30: Good practice – Testen business rules

Een instelling documenteert op welke wijze zij tot een definitie van een business rule is gekomen, hoe ze doorlopend haar business rules onderhoudt en hoe ze de rules periodiek test met behulp van backtesting. Met de uitkomsten van de backtests toetst de instelling de effectiviteit van de toegepaste business rules en past deze waar nodig aan.

## GP4.31: Good practice – Testen

Een instelling houdt de business rules en de instellingen van het transactiemonitoringsysteem actueel en test deze structureel. De instelling legt de tests en de uitkomsten daarvan vast.

Ook monitort de instelling op basis van management informatie of de output van de verschillende business rules en modellen (bijv. in de vorm van aantallen alerts, FIU-meldingen en bijbehorende bedragen) aansluit bij de in de risicoanalyse (SIRA) geïdentificeerde risico's. Een te beperkte output van het transactiemonitoringsysteem geeft de instelling inzicht in welke business rules en modellen onvoldoende de inherente risico's in de portefeuille oppikken en of er aanvullende maatregelen moeten worden getroffen.

De instelling legt de resultaten van deze analyses alsook de analyse en overwegingen hieromtrent vast. De instelling heeft verder de structurele inrichting van het *quality assurance framework* en de periodieke *above- and below the line testing* gedocumenteerd. Waar nodig voert de instelling aanpassingen door naar aanleiding van de uitkomsten van de testen.

Ook gebruikt de instelling de getrokken lessen uit FIU-meldingen, incidenten, thematische onderzoeken en cliëntreviews om te bezien of de risicoanalyse nog actueel is, en of het transactiemonitoringsysteem herijkt zou moeten worden.

## GP4.32: Good practice – Feedback-loop

Een instelling beschikt over een systeem dat periodiek de effectiviteit van alle business rules evalueert en uit een ruime set aan variabelen een overzicht creëert van de variabelen die de business rules potentieel verbeteren. In de periodieke controle is een business rule op internationale transacties omhoog gekomen met veel meer *false positives* op transacties binnen de EU dan op transacties buiten de EU.

De bank heeft deze waarneming aangevuld met een data- en risicoanalyse, om te na te gaan of bij potentiële aanpassingen de business rule het beoogde risico nog voldoende afdekt. Vervolgens heeft de bank een aanpassing gedaan in de business rule door de grenswaarde voor transacties binnen de EU op te hogen ten opzichte van de grenswaarde voor transacties buiten de EU.
De feedback-loop heeft zo geleid tot een business rule met een hogere effectiviteit.

## GP4.33: Good practice – Gebruik maken van FIU-data en typologieën

Een instelling heeft een procedure die ervoor zorgt dat de risicoanalyse wordt geactualiseerd met als input de FIU-meldingen en de terugmeldingen van FIU-NL. Andere bronnen, zoals typologieën en recente ontwikkelingen, worden ook betrokken bij de herijking van de risicoanalyse.

Aan de hand van de bijgewerkte risicoanalyse bekijkt de instelling ook de gebruikte business rules en modellen en past deze waar nodig aan.

### GP4.34: Good practice – Identificatie false negatives

Naar aanleiding van een publicatie over een witwaszaak gaat een bank de betalingen na die naar een land in het Midden-Oosten zijn gedaan. Het blijkt dat enkele cliënten in korte tijd veel transacties naar dit land in het Midden-Oosten hebben gedaan.

De bank ziet ook dat het transactiemonitoringsysteem geen alerts heeft gegenereerd op deze transacties. De bank vindt dit ongewenst en past de business rules aan zodat dergelijke transacties wel zullen worden opgemerkt.

## 4.2 Review van de cliënt

Een review van de cliënt is van belang om het risicoprofiel en de onderliggende gegevens actueel te houden. Op basis daarvan kan de instelling nagaan of de cliënt nog past binnen de risicotolerantie en of er aanvullende maatregelen nodig zijn dan wel of er volstaan kan worden met minder maatregelen.

Een review van de cliënt kan plaatsvinden n.a.v. het verstrijken van een periode (periodieke review) en/of n.a.v. het optreden van gebeurtenissen/signalen/alerts ('event-driven review'). Deze alerts kunnen bijvoorbeeld ontstaan vanuit de transactiemonitoring, wijzigingen in de gegevens van de cliënt en vanuit externe bronnen.

### Q&A

**QA4.35: Vraag**

Wanneer is een review van belang?

**Antwoord**

Een review is met name van belang als er sprake is van een hoger risico of als er signalen zijn dat het risicoprofiel van de cliënt is gewijzigd. Een review is onder andere aan de orde:[183]

- indien er indicaties zijn dat de cliënt betrokken is bij witwassen of financieren van terrorisme
- indien de instelling twijfelt aan de juistheid of volledigheid van eerder verkregen gegevens van de cliënt
- indien het risico van betrokkenheid van een cliënt bij witwassen of financieren van terrorisme daartoe aanleiding geeft.

De instelling neemt redelijke maatregelen om de gegevens van de cliënt actueel te houden.[184]
De gegevens met betrekking tot de cliënt worden in elk geval geactualiseerd indien relevante omstandigheden van de cliënt veranderen. Hierbij kan onder meer gedacht worden aan opmerkelijk en afwijkend transactiegedrag of indien een cliënt deel uit gaat maken van een andere of gewijzigde eigendoms- of zeggenschapsstructuur. Ook kan gedacht worden aan signalen die een instelling ontvangt vanuit bijvoorbeeld de cliënt zelf, uit rechtszaken en uit de pers.

183 Art. 3 lid 5 Wwft.
184 Art. 3 lid 11 Wwft, art. 6 lid 3 Wwft, art. 8 lid 11 Wwft.

**QA4.36: Vraag**
In hoeverre is er bij een review sprake van klantcontact?

**Antwoord**
Het doel van de review is om te bepalen of het risicoprofiel nog actueel is en om waar nodig de gegevens met betrekking tot de cliënt te actualiseren. Op basis hiervan kan de instelling bepalen of het niveau van beheersing nog passend is. Afhankelijk van het risico en de signalen kan de instelling volstaan met het raadplegen en analyseren van interne en externe bronnen. Klantcontact zal niet in alle gevallen nodig zijn.

**QA4.37: Vraag**
Wat is het resultaat van de cliëntreview?

**Antwoord**
Na de cliëntreview beschikt de instelling over een actueel en goed vastgelegd cliëntendossier dat voldoet aan de vereisten. De instelling heeft ook het risicoprofiel van de cliënt geactualiseerd.

**QA4.38: Vraag**
Welke maatregelen kunnen volgen uit een review?

**Antwoord**
De uitkomst van de review kan aanleiding zijn voor onder meer de volgende maatregelen:

- De instelling neemt afscheid van de cliënt. Dit speelt met name in de volgende gevallen:
  - Een instelling kan op basis van de review/ het cliëntenonderzoek concluderen dat een cliënt te grote integriteitrisico's met zich brengt.
  - Het cliëntenonderzoek in het kader van de review kan mislukken – bijvoorbeeld door het ontbreken van noodzakelijke informatie – waardoor de instelling niet (meer) kan vaststellen wie haar cliënt precies is en/of wie de UBO's zijn en/of welk doel de zakelijke relatie heeft, en/of de beoogde dienstverlening passend is.[185]
- De instelling neemt verscherpte maatregelen met betrekking tot de cliënt, zoals het beperken van de dienstverlening.
- De instelling verlaagt het niveau van beheersing omdat het risicoprofiel van de cliënt lager is dan voorheen.
- Als de instelling op basis van de review vaststelt dat er sprake is geweest van een of meer ongebruikelijke transacties dan meldt zij deze transacties meteen nadat het ongebruikelijke karakter hiervan bekend is geworden, aan de FIU.[186]

185 Art. 5 lid 3 Wwft.
186 Art. 16 lid 1 Wwft.

**QA4.39: Vraag**
In hoeverre moet een instelling de cliëntrelatie opzeggen na een vordering van het OM?

**Antwoord**
Instellingen kunnen geconfronteerd worden met een vordering van het OM om cliëntinformatie te verstrekken in het kader van een strafrechtelijk onderzoek. De instelling kan informatie m.b.t. de vordering niet delen met haar cliënten.

Een vordering kan voor de instelling aanleiding zijn om nader (verscherpt) cliëntenonderzoek in te stellen en de transacties van de cliënt extra te monitoren. De uitkomst van het nadere cliëntenonderzoek kan voor instellingen aanleiding zijn om aanvullende beheersmaatregelen te treffen of om ongebruikelijke transacties te melden aan de FIU, overigens zonder de vordering te bespreken met de cliënt.

Wanneer het OM vanwege het onderzoek niet wil dat de cliënt op enige wijze te weten komt dat er een onderzoek loopt, dan zal dat expliciet bij de vordering worden aangegeven. Dit betekent dat indien de instelling beheersmaatregelen treft deze door de cliënt niet in verband kunnen worden gebracht met een actie van het OM.

Een vordering van het OM hoeft voor een instelling geen aanleiding te zijn om de cliëntrelatie op basis van de Wwft of Wft te beëindigen of de dienstverlening op te schorten. Een instelling kan op basis van door haar verricht cliëntenonderzoek tot de conclusie komen dat de cliënt onacceptabele risico's meebrengt en dat er grond bestaat om afscheid te nemen van de cliënt. Indien sprake is van onacceptabele risico's of indien niet kan worden voldaan aan de eisen van het cliëntenonderzoek, dient de instelling de cliëntrelatie bij de eerstvolgende mogelijkheid te verbreken.

Echter, indien het strafrechtelijk onderzoek vergt dat de cliëntrelatie en de transacties worden gecontinueerd, dan kan de cliëntrelatie niet beëindigd worden. Het verzoek om de cliëntrelatie en de transacties te continueren zal door de Officier van Justitie, bij de vordering, worden gedaan. In die situatie bieden een verscherpte monitoring van de cliënt en zijn transacties, en een zorgvuldige vastlegging van de relevante feiten en omstandigheden in het cliëntendossier waarborgen om mogelijke risico's te mitigeren. Instellingen mogen in een dergelijk geval alleen afscheid nemen van een cliënt wanneer het OM toestemming geeft.

## GP4.35: Good practice Review

Een instelling voert bij een review ten minste de volgende acties uit:
- Check op sancties en PEP. Bij hoge risico s wordt ook een check gedaan op 85 bad press .
- Analyse van de transacties van de cliënt, waarbij wordt nagegaan:
  - of transacties passen binnen doel en aard van de relatie
  - of de transacties in lijn zijn met de bron van de middelen die bij de zakelijke relatie of de transactie gebruikt worden
  - of er sprake is van opvallende transacties of transactiepatronen, waarbij de instelling betrekt de hoogte van bedragen en ongebruikelijk veel cash transacties, bedragen die gelijk worden doorgestort naar een andere rekening, mogelijk gebruik van de rekeningen door derden, en onbekende tegenpartijen.

Transacties die hierbij opvallen en niet direct kunnen worden verklaard, worden nader geanalyseerd. Ten behoeve van deze analyse wordt zo nodig nadere informatie ingewonnen bij de betreffende cliënt, bijvoorbeeld over de bron van de middelen.
- Actualiseren van de cliëntgegevens, waaronder de UBO-gegevens.
- Actualiseren van het risicoprofiel. De actualisering van het risicoprofiel kan gevolgen hebben voor de toe te passen mitigerende maatregelen.

De instelling heeft in de reviewprocedure vastgelegd dat de verzamelde informatie een gedegen onderbouwing van de analyse, het risicoprofiel en het gekozen niveau van beheersing moet vormen.

## GP4.36: Good practice Cliëntexitbeleid

Om te waarborgen dat op een adequate manier afscheid kan worden genomen van bestaande cliënten, heeft de instelling een cliëntexitbeleid opgesteld. Hierin geeft zij aan onder welke omstandigheden en volgens welke procedure (inclusief de te hanteren termijnen) de relatie met de cliënt wordt beëindigd. De instelling monitort de voortgang van het exittraject van de betreffende cliënten en onderneemt actie als hierbij de afgesproken tijdlijnen worden overschreden.

## GP4.37: Good practice Aanvullende informatie en exit

Tijdens de review blijkt dat de cliënt als PEP kwalificeert. De instelling neemt daarop de in haar beleid uitgewerkte extra maatregelen en vraagt in dat kader aanvullende informatie op. De cliënt weigert deze te verstrekken, waarop de instelling de dienstverlening beperkt en de exitprocedure start.

## GP4.38: Good practice Beperken dienstverlening

Een bank signaleert dat een cliënt de private banking rekening gebruikt voor zakelijke doeleinden. Op basis van een nader onderzoek, met navraag bij de cliënt, kan de bank geen sluitende positieve conclusie trekken over de herkomst van de gelden op de private banking rekening. De cliënt heeft ook een betaalrekening, en ten aanzien van deze rekening zijn er geen twijfels over de geldstromen.

De bank besluit om de private banking rekening te sluiten. De cliënt kan de betaalrekening behouden. De bank past op deze rekening wel een verscherpt regime toe. Dit regime houdt onder meer in dat betalingen vanaf 2.000 euro in een aparte verwerking komen, waarbij deze vooraf door de bank worden bekeken en goedgekeurd alvorens ze verder verwerkt worden.

## GP4.39: Good practice Relevante gegevens

De instelling heeft per risicocategorie vastgelegd welke gegevens relevant zijn voor de vastgestelde risico s en hoe vaak de gegevens in het clientdossier geactualiseerd moeten worden. Op basis hiervan heeft de instelling haar reviewprocedure ingericht.

## GP4.40: Good practice Periodiciteit bepalen

De instelling heeft per risicocategorie de periodiciteit van de review vastgelegd. Voor lagere risico s hanteert de instelling een systeem van 86 event-driven review , dat wil zeggen dat de instelling in die gevallen alleen overgaat tot een review als er signalen zijn (vanuit externe bronnen, interne bronnen/transacties of vanuit informatie uit klantcontact) dat het risicoprofiel is gewijzigd dan wel dat de cliëntgegevens niet actueel zijn.

De instelling heeft vastgelegd dat een review in ieder geval aan de orde is op het moment dat:
- de cliënt een nieuwe dienst of product vraagt
- er signalen zijn dat de cliënt is verhuisd naar een hoog-risico jurisdictie
- de cliënt een PEP wordt.

De instelling heeft in haar bedrijfsvoering, onder meer in haar proces van transactiemonitoring, geborgd dat signalen tijdig naar boven komen. De instelling test periodiek de werking hiervan. De compliancefunctie houdt hier toezicht op.

Voor hoge risico s hanteert de instelling ten minste een periodieke review, naast een 86 event-driven review in het geval er signalen zijn.

## GP4.41: Good practice Afspraken met cliënt

Een instelling heeft contractueel vastgelegd dat de cliënt wisselingen in het bestuur en in de aandeelhouders direct meldt aan de instelling.

Daarnaast heeft de instelling een trigger ingebouwd in het systeem om bestuurswisselingen te kunnen identificeren, waarbij gebruik wordt gemaakt van een koppeling met de Kamer van Koophandel. Bij hoog-risicocliënten gaat de instelling periodiek na of de UBO-informatie actueel is.

# Bijlage I Afkortingenlijst

| | |
|---|---|
| **(A)ML** | (Anti) Money Laundering |
| **(C)FT** | (Counter) Financing of Terrorism |
| **AMLD** | Anti-Money Laundering Directive, of antiwitwasrichtlijn. |
| **AP** | Autoriteit Persoonsgegevens |
| **AVG** | Algemene Verordening Gegevensbescherming |
| **Bpr** | Besluit prudentiële regels |
| **BSN** | Burgerservicenummer |
| **CDD** | Customer Due Diligence, of cliëntenonderzoek |
| **EBA** | European Banking Authority, of Europese Bankenautoriteit |
| **EDD** | Enhanced Due Diligence |
| **eID** | Elektronisch identificatiemiddel |
| **eIDAS** | Electronic Identities and Trust Services (verordening) |
| **ETP** | Expected Transaction Profile, of verwacht transactieprofiel |
| **FATF** | Financial Action Task Force |
| **FIU** | Financial Intelligence Unit, of Financiële inlichtingen eenheid |
| **HRTC** | High Risk Third Country, of hoog risico derde land |
| **MiCAR** | Markets in Crypto Assets Regulation |
| **OM** | Openbaar Ministerie |
| **PEP** | Politically Exposed Person, of politiek prominent persoon |
| **SIRA** | Systematische Integriteitsrisicoanalyse |
| **SME/MKB** | Small and medium enterprises, midden- en kleinbedrijf |
| **TFR** | Transfer of Funds Regulation |
| **UBO** | Ultimate beneficial owner, of uiteindelijk belanghebbende |
| **Wft** | Wet op het financieel toezicht |
| **WTR(2)** | Wire Transfer Regulation |
| **Wtt 2018** | Wet toezicht trustkantoren 2018 |
| **Wwft** | Wet ter voorkoming van witwassen en financieren van terrorisme |

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

Volg ons op:

DeNederlandscheBank
EUROSYSTEEM