

Compliance Week AML Syllabus 2026

April 20 - 24, 2026



Inhoudstafel

Inleiding	3
Hoofdstuk 1: AML in de Antwerpse diamantindustrie	4
Hoofdstuk 2: Wettelijke verplichtingen binnen de AML-wetgeving	10
Hoofdstuk 3: Know Your Counterparty (Client of Supplier)	16
Hoofdstuk 4: Risicobehoordeling en hoogrisicosituaties	24
Hoofdstuk 5: Melden van verdachte activiteiten	45
Hoofdstuk 6: Hoe bereid je je voor op een AML-controle?	51
Hoofdstuk 7: AML Templates, tools en manuals aangeboden door AWDC	56
Woordenlijst	62
Annex	69

Inleiding

Anti-witwas (AML) is een belangrijk onderwerp voor bedrijven in de diamantsector. De Belgische overheid houdt strikt toezicht op de naleving van de AML-wetgeving en hecht groot belang aan de kennis van en de naleving van deze regels binnen de sector.

Als sectorfederatie streeft AWDC ernaar Antwerpse diamantbedrijven zo goed mogelijk te ondersteunen en te begeleiden bij een efficiënte en correcte naleving van de toepasselijke regelgeving. Met deze syllabus willen we de vaak complexe AML-wetgeving vertalen naar de dagelijkse praktijk en de nodige kennis op een toegankelijke manier aanbieden.

Vanaf 2026 zal de Belgische overheid voor het eerst een grootschalig fysiek AML-examen organiseren. Het doel van deze syllabus is om diamantbedrijven hierop optimaal voor te bereiden. Aan het einde van elk hoofdstuk kan u uw kennis testen aan de hand van voorbeeldvragen, gebaseerd op input van de Federale Overheidsdienst Economie (FOD Economie) en representatief voor mogelijke examenvragen.

Wij wensen u veel succes en een aangename leerervaring!

Hoofdstuk 1: AML in de Antwerpse diamantindustrie

Wat leer ik in dit hoofdstuk?

1.1 Wat is AML?

1.2 Waarom is het belangrijk om AML-compliant te zijn?

1.3 Hoe ziet een AML-traject eruit binnen een diamantbedrijf?

De antiwitwas (AWW)-wetgeving – in het Engels Anti-Money Laundering (AML) genoemd – heeft tot doel witwassen en de financiering van terrorisme te voorkomen. In het geval van witwassen is het doel om de illegale oorsprong van fondsen te verbergen, terwijl bij terrorismefinanciering het doel is om de illegale bestemming ervan te verhullen.

AML bestaat uit een geheel van wettelijke regels en procedures die diamantbedrijven (evenals andere gereguleerde entiteiten en sectoren zoals financiële instellingen, vastgoedmakelaars, professionele voetbalclubs, enz.) verplichten om verdachte financiële stromen te detecteren en te melden.

De antiwitwaswetgeving is niet nieuw; zij is al vele jaren van kracht. Met de wet van 12 januari 2004 werd de diamantsector officieel onderworpen aan preventieve verplichtingen ter bestrijding van het witwassen van geld. Naast het wettelijke kader en de verplichtingen is AML uitgegroeid tot een integraal onderdeel van moderne bedrijfsvoering, waarbij bedrijven geholpen worden om bepaalde risico's te beperken. Bovendien wordt AML-wetgeving niet alleen in België toegepast, maar in de belangrijkste financiële markten wereldwijd geïmplementeerd.

Drie organisaties spelen een belangrijke rol in AML voor diamantbedrijven in België:

- FOD Economie – controleert diamantbedrijven en gaat na of de AML-regels worden nageleefd
- AWDC – ondersteunt diamantbedrijven met praktische tools, templates en opleidingen
- CFI – ontvangt en analyseert meldingen van verdachte transacties

Het huidige AML-kader bestaat uit:

- AML-wet (2017) – de algemene Belgische wet inzake witwassen
 - Bijgewerkt bij Koninklijk Besluit van 17 maart 2024
- Koninklijk Besluit (2019) – specifieke AML-regels voor de diamantsector

De diamantsector is bijzonder kwetsbaar voor witwassen door kenmerken zoals:

- Hoge waarde en klein formaat van diamanten: het zijn waardevolle goederen die zeer gemakkelijk en discreet kunnen worden vervoerd.
- Internationaal en weinig transparant karakter: de handel is sterk internationaal. Veel diamantbedrijven werken via internationale structuren, met dochterondernemingen in meerdere landen en vrijhandelszones (zoals Dubai), waar het toezicht soms beperkt kan zijn.

- Ondanks steeds strengere regelgeving steunen sommige delen van de waardeketen buiten Antwerpen nog steeds op informele handelspraktijken en contante betalingen, wat de controle bemoeilijkt.

→ Dit maakt diamanten aantrekkelijk voor personen met criminele of illegale intenties als middel om financiële stromen te verbergen of te verplaatsen.

1.2 Waarom is het belangrijk om AML-compliant te zijn?

- Alle handelaren in diamanten en/of synthetische diamanten,
- makelaars en producenten die diamanten en/of synthetische diamanten gebruiken bij de
- vervaardiging van apparatuur,
- zelfstandigen en ondernemingen, die onder Belgisch of buitenlands

recht vallen, op voorwaarde dat zij een filiaal of dochteronderneming in België hebben

1.3 Waarom is het belangrijk om AML-compliant te zijn?

Voor uw bedrijf

- Als diamanthandelaar bent u wettelijk verplicht om de AML-regelgeving na te leven.
 - Bij overtredingen kunnen administratieve boetes van € 250 en € 1.250.000 worden opgelegd.
 - De boetes worden opgelegd door de FOD Economie en geïnd door de FOD
- Financiën.
- In geval van inbreuken kunnen boetes tot €1.250.000 worden opgelegd.
- Daarnaast riskeert u reputatieschade en het verlies van zakenpartners indien u de wetgeving niet naleeft.
- U zou bovendien – onbewust – terroristische organisaties kunnen helpen (iets wat u uiteraard wil vermijden).

Voor de Antwerpse diamantsector

- De naleving door elke individuele onderneming heeft een directe impact op de volledige sector. Om de vijf jaar evalueert de Financial Action Task Force (FATF) hoe kwetsbaar een land is voor witwassen.

Een slecht FATF-rapport leidt tot:

- Strengere regelgeving en meer overheidscontroles
- Verminderd vertrouwen van banken
- Verminderd vertrouwen van mijnbedrijven en internationale klanten (zoals juwelenmerken)

Sterke naleving daarentegen leidt tot:

- Groter vertrouwen van banken en financiële instellingen
- Groter vertrouwen van internationale partners
- Een sterke reputatie voor Antwerpen als het meest betrouwbare diamant-handelscentrum ter wereld

Voordat u een nieuwe zakelijke relatie of transactie aangaat, moet u een aantal verplichte stappen volgen.

Samen vormen deze stappen het AML-traject, dat van toepassing is op elke klant, leverancier en transactie. **Meer dan 10.000 euro of meer dan één transactie van minder dan 10.000 euro.**

Stap 1: Organisatorische verplichtingen

Voordat u een zakelijke relatie aangaat met een potentiële klant of leverancier, moet u als geregistreerd diamantbedrijf voldoen aan een aantal wettelijke en organisatorische verplichtingen:

- Beschikken over een intern AML-beleid;
- Minstens één AML-verantwoordelijke aanstellen;
- Jaarlijks het AML-webinar volgen of slagen voor het AML-examen, dat vanaf 2026 om de drie jaar door de overheid zal worden georganiseerd;
- Een jaarlijks AML-verslag indienen bij de autoriteiten.

Stap 2: KYC (Know Your Counterparty)

Zodra uw bedrijf voldoet aan alle organisatorische verplichtingen, bent u klaar om een eerste zakelijke relatie aan te gaan met een klant of leverancier.

Voordat u effectief zaken doet, moet u echter alle AML-gerelateerde informatie over uw tegenpartij verzamelen, de juistheid ervan verifiëren en ervoor zorgen dat deze up-to-date blijft.

Dit proces wordt KYC (Know Your Counterparty) genoemd. Kort gezegd: weet altijd met wie u zaken doet, vóórdat u zaken doet.

Stap 3: Risicoanalyse

Op basis van de informatie die u tijdens het KYC-proces over uw tegenpartij hebt verzameld, moet u een risicoanalyse uitvoeren waarin u beoordeelt hoe veilig of risicovol het is om met deze partij zaken te doen.

U kunt deze risicoanalyse manueel uitvoeren met behulp van risicoscorekaarten of digitaal via het KYCP-platform. Tijdens dit proces kent u een risicocategorie toe aan uw tegenpartij (laag, middel of hoog) en zorgt u ervoor dat deze informatie continu up-to-date blijft. Indien er relevante wijzigingen optreden, zoals veranderingen in de aandeelhoudersstructuur van de tegenpartij, moet de risicoanalyse opnieuw worden uitgevoerd.

Stap 4: Beslissen om de zakelijke relatie al dan niet aan te gaan

Het resultaat van de risicoanalyse toont aan of het veilig en wettelijk toegestaan is om zaken te doen. Op basis hiervan beslist u om de relatie te aanvaarden, te aanvaarden onder bepaalde voorwaarden, of te weigeren of te beëindigen.

Stap 5: Melden van verdachte situaties

Tijdens het volledige AML-proces kunnen zich verdachte situaties voordoen, bijvoorbeeld een klant die aandringt op het betalen van grote bedragen in contanten, snel wil handelen en het KYC-proces wil overslaan, of een tegenpartij die onvolledige, tegenstrijdige of duidelijk onjuiste informatie verstrekt over haar identiteit, haar bedrijf of de uiteindelijke begunstigden van de onderneming ("UBO").

Zodra iets ongebruikelijk of verdacht lijkt, moet u dit melden aan de Cel voor Financiële Informatieverwerking (CFI), zelfs als u geen concreet of tastbaar bewijs hebt van fraude of witwassen en het slechts om een vermoeden gaat.

Praktisch voorbeeld:

U bent een diamanthandelaar in Antwerpen en wordt gecontacteerd door een nieuwe internationale klant gevestigd buiten Europa. Hij toont interesse in een partij diamanten en wil snel handelen. Op het eerste gezicht lijkt alles aantrekkelijk, tot hij aangeeft dat hij de goederen in contanten wil betalen.

Op dat moment begint uw AML-traject. U kan de deal niet zomaar accepteren, hoe aantrekkelijk die ook lijkt. Eerst moet u weten met wie u te maken heeft. U verzamelt informatie over de klant (= KYC-proces): wie is hij, welk bedrijf vertegenwoordigt hij en waar komt het geld vandaan? U verifieert deze informatie en controleert of alles correct is.

Vervolgens voert u een risicoanalyse uit: u gaat na of het veilig en wettelijk toegestaan is om met deze partij zaken te doen. Een internationale klant buiten Europa die snel wil handelen en in contanten wil betalen voor diamanten van hoge waarde: dit zijn duidelijke risicofactoren. U beoordeelt deze elementen en bepaalt of het risico laag, middel of hoog is. Hier bevinden we ons in een hoogriscosituatie.

Op basis hiervan neemt u een beslissing: gaat u verder met de transactie, legt u bijkomende voorwaarden op (bijvoorbeeld geen contante betaling), of weigert u de transactie volledig? Als iets niet klopt of het risico te hoog is, moet u niet alleen het proces stopzetten, maar dit ook melden aan de Cel voor Financiële Informatieverwerking.

Dit is hoe AML er in de praktijk uit ziet: geen theoretische oefening, maar een reeks weloverwogen stappen die u neemt om uzelf, uw bedrijf en de volledige Antwerpse diamantsector te beschermen.

Test uw kennis

(juiste antwoorden worden aan het einde van deze syllabus gegeven)

1. Wat is het maximumbedrag van de boete voor een rechtspersoon onder de Belgische antiwitwaswetgeving in geval van niet-naleving door een diamanthandelaar?
 - a. 1.000.000 euro
 - b. 2.000.000 euro
 - c. 3.000.000 euro
 - d. 1.250.000 euro

2. Welke Belgische overheidsdienst is verantwoordelijk voor het uitvoeren van AML-controles?
 - a. FOD Financiën
 - b. CFI
 - c. FOD Economie

Hoofdstuk 2: Wettelijke verplichtingen binnen de AML-wetgeving

Wat leer ik in dit hoofdstuk?

2.1 Wat zijn de wettelijke verplichtingen voor diamantbedrijven binnen de AML-wetgeving?

2.1

Wat zijn de wettelijke verplichtingen voor diamantbedrijven binnen de AML-wetgeving?

De antiwitwas (AML)-wetgeving legt een breed scala aan verplichtingen op aan diamantbedrijven. Als diamanthandelaar bent u wettelijk verplicht om doeltreffende maatregelen te nemen om witwassen en de financiering van terrorisme te voorkomen.

Als diamantbedrijf heeft u vier belangrijke wettelijke verplichtingen onder de AML-wetgeving. Elk van deze verplichtingen is verplicht.

1. Beschikken over een schriftelijk AML-beleid
2. Eén of meerdere AML-verantwoordelijken aanstellen
3. Slagen voor het AML-examen om de drie jaar, of jaarlijks het AML-webinar volgen
4. Een jaarlijks AML-verslag indienen bij de FOD Economie

In de volgende subhoofdstukken gaan we specifiek in op deze organisatorische verplichtingen, met andere woorden, hoe uw bedrijf moet worden gestructureerd en beheerd om volledige AML-naleving te waarborgen.

2.1.1 Beschikken over een intern AML-beleid (verplicht)

Elk diamantbedrijf moet beschikken over een robuust en schriftelijk intern AML-beleid.

Dit beleid legt uit hoe uw onderneming voldoet aan de AML-verplichtingen en moet worden aangepast aan uw specifieke bedrijfsactiviteiten.

Het AML-beleid moet minimaal het volgende bevatten:

- Procedures voor het identificeren en verifiëren van uw klanten en leveranciers (KYC)
- Procedures voor het uitvoeren van risicoanalyses
- Procedures om uw AML-gegevens up-to-date te houden
- Procedures voor het melden van verdachte activiteiten aan de CFI
- De namen van de personen die verantwoordelijk zijn voor (de naleving van) AML binnen uw onderneming (AML-verantwoordelijken)
- Procedures voor archivering en documentatievereisten

Opgelet

Het beleid moet up-to-date worden gehouden en beschikbaar zijn tijdens AML-controles.

AWDC stelt een template ter beschikking dat is goedgekeurd door de FOD Economie en dat bedrijven kunnen aanpassen aan hun eigen situatie. Wij raden alle Belgische diamantbedrijven aan om gebruik te maken van deze template:



2.1.2 Een AML-verantwoordelijke aanstellen (verplicht)

Elk diamantbedrijf moet minstens één AML-verantwoordelijke aanstellen. **Eén AML-functionaris op managementniveau en eventueel een extra functionaris op uitvoerend niveau.** Er zijn twee rollen:

- De eindverantwoordelijke voor AML is een persoon op senior managementniveau die ervoor zorgt dat het bedrijf de AML-wetgeving naleeft. Indien u zelfstandige bent, vervult u deze rol zelf.
- De operationele AML-verantwoordelijke wordt aangesteld door het senior management. Deze persoon behandelt AML in de dagelijkse werking. Hij of zij zorgt ervoor dat de AML-regels worden nageleefd, controleert risico's, monitort tegenpartijen, leidt personeel op en meldt verdachte activiteiten. Indien u zelfstandige bent, vervult u ook deze rol zelf. **De uitvoerende functionaris is optioneel.**

De operationele AML-verantwoordelijke is verantwoordelijk voor:

- Het naleven van de AML-wetgeving
- Het uitvoeren van KYC en risicoanalyses
- Het monitoren van zakelijke relaties
- Het melden van verdachte activiteiten aan de CFI
- Het opleiden van personeel inzake AML
- Het behalen van een AML-certificaat elk jaar (webinar) of om de drie jaar (examen)
- Het opstellen en onderhouden van het AML-beleid van het bedrijf
- Het indienen van het jaarlijkse AML-verslag

Opgelet

Tijdens een inspectie moet het onmiddellijk duidelijk zijn wie de uiteindelijke AML-verantwoordelijke is en wie de rol van operationele AML-verantwoordelijke vervult.

AML-verantwoordelijken moeten officieel geregistreerd worden bij de FOD Economie door de namen van de AML-verantwoordelijken te vermelden in het jaarlijkse AML-verslag.

Het is goede praktijk om de aanstelling van AML-verantwoordelijken formeel vast te leggen in de notulen van een bestuursvergadering. Officiële registratie is bovendien vereist om te kunnen deelnemen aan het fysieke AML-examen.

2.1.3 Het driejaarlijkse AML-examen afleggen of jaarlijks het AML-webinar volgen (verplicht)

Om aan te tonen dat er binnen uw onderneming voldoende kennis is van de AML-wetgeving, moet minstens één van de officiële AML-verantwoordelijken een AML-certificaat behalen.

Dit kan op twee manieren:

- Deelnemen aan en slagen voor het grootschalige fysieke AML-examen, dat om de drie jaar wordt georganiseerd door de FOD Economie. Meer informatie: www.awdc.be/aml-exam.
- Jaarlijks het AML-webinar volgen en vervolgens de bijhorende vragenlijst succesvol afronden via www.MyAWDC.be.

In beide gevallen ontvangt u een AML-certificaat na het slagen voor het examen of de vragenlijst na het webinar.

Opgelet

Het AML-certificaat is een belangrijk en verplicht onderdeel van uw jaarlijkse AML-verslag (zie hoofdstuk 2.1.4 – Dien uw jaarlijks AML-verslag in bij de FOD Economie).

Bewaar het certificaat op de maatschappelijke zetel van uw onderneming. U moet het kunnen voorleggen tijdens een AML-controle.

Elke onderneming moet ervoor zorgen dat minstens één van haar AML-verantwoordelijken een AML-certificaat behaalt, hetzij door het volgen van het AML-webinar, hetzij door te slagen voor het AML-examen.

2.1.4 Dien uw jaarlijks AML-verslag in bij de FPS Economy (verplicht)

Elk jaar moet u een AML-verslag over het voorgaande jaar indienen bij de FPS Economy via:



Het verslag omvat:

- De identiteit van uw onderneming
- Uw AML-organisatie en procedures
- Hoe u KYC en risicoanalyses hebt toegepast
- Eventuele verdachte activiteiten die u hebt gemeld aan de CFI
- Hoe u de sanctieregels naleeft

Opgelet

De uiterste deadline voor het indienen van dit AML-verslag is 31 maart (elk jaar).

Alleen (één van) de AML-verantwoordelijke(n) is/zijn bevoegd om het jaarlijkse AML-verslag op te stellen, te ondertekenen en in te dienen.

Deze handleiding begeleidt u stap voor stap door het proces voor het indienen van het AML-verslag:



Test uw kennis

(juiste antwoorden worden aan het einde van deze syllabus gegeven)

1. Wat is de deadline voor het indienen van het jaarlijkse AML-verslag?
 - a. 1 april
 - b. 31 maart
 - c. 31 mei
 - d. 1 juni

2. Hoe vaak moet u een AML-opleiding volgen als u niet geslaagd bent voor het AML-examen?
 - a. Elk jaar
 - b. Om de twee jaar
 - c. Om de drie jaar
 - d. Om de vier jaar

3. Een AML-verantwoordelijke kan zelfstandig beslissen om bedrijfsmiddelen te gebruiken om aan AML-verplichtingen te voldoen.
 - a. Juist
 - b. Onjuist

4. Alleen de AML-verantwoordelijke (of de door het management aangestelde persoon) kan het jaarlijkse AML-verslag opstellen.
 - a. Juist
 - b. Onjuist

5. Welke Belgische overheidsinstantie houdt toezicht op EU-financiële sancties?

6. Hoeveel keer per jaar moet u een AML-opleiding volgen als u niet geslaagd bent voor het examen? (Geef een getal)

Hoofdstuk 3: Know Your Counterparty (KYC)

Wat leer ik in dit hoofdstuk?

3.1 Wat is KYC en AML-gegevensverzameling en waarom is dit belangrijk?

3.2 Verzamelen en verifiëren van AML-gegevens

3.3 Actualiseren en onderhouden van AML-gegevens

3.4 GDPR-overwegingen en non-compliance

3.5 Voortdurende waakzaamheid tijdens de zakelijke relatie

3.1 Wat is KYC en AML-gegevensverzameling en waarom is dit belangrijk?

Het doel van Know Your Counterparty (KYC) is het voorkomen van witwassen en terrorismefinanciering door te begrijpen wie uw tegenpartijen zijn. KYC zorgt ervoor dat uw onderneming niet onbewust illegale activiteiten faciliteert.

KYC — Know Your Counterparty — betekent het verzamelen en verifiëren van informatie over de personen en bedrijven waarmee u zaken doet, voordat u met hen begint samen te werken.

Het doel is eenvoudig: weten met wie u zaken doet.

KYC stelt u in staat om:

- Te bevestigen wie uw klant of leverancier werkelijk is
- In te schatten hoe risicovol het is om met hen samen te werken
- Ongebruikelijk of verdacht gedrag te detecteren
- Te beschikken over de nodige informatie indien u moet rapporteren aan de CFI

3.2 Verzamelen en verifiëren van AML-gegevens

3.2.1 Wanneer en van wie AML-gegevens verzamelen en verifiëren

U moet KYC-informatie verzamelen in de volgende situaties:

- Vóór het aangaan van elke zakelijke relatie — met een nieuwe klant of leverancier
- **OF** Vóór een eenmalige transactie van €10.000 of meer — zelfs als er geen doorlopende relatie is

Uitzondering

Indien de eerste transactie met een nieuwe tegenpartij onder €10.000 ligt, is KYC niet vereist — tenzij er een tweede gerelateerde transactie volgt, of tenzij de tegenpartij een hoog risico vormt (bijvoorbeeld een PEP of iemand uit een hoogrisicoland).

U bent verantwoordelijk om ervoor te zorgen dat de informatie over uw tegenpartij correct, up-to-date en volledig is, en dat dit zo blijft gedurende de volledige zakelijke relatie. Informatie moet minstens jaarlijks worden bijgewerkt voor tegenpartijen met een hoog risico, en om de 2-3 jaar voor tegenpartijen met een laag risico (infra).

3.2.2 Wat zijn de identificatievereisten?

Voor een persoon (natuurlijke persoon):

- Volledige naam
- Geboortedatum en -plaats
- Adres (indien mogelijk)
- Kopie van een geldig identiteitsbewijs (paspoort of identiteitskaart)

Voor een onderneming:

- Bedrijfsnaam en rechtsvorm (bijv. NV, BV, Ltd)
- Geregistreerd adres
- Lijst van bestuurders
- Uiteindelijke begunstigen (UBO's) — zie sectie 3.2.2.1

3.2.2.1 Identificatie van uiteindelijke begunstigen (UBO's)

UBO's zijn de natuurlijke (echte) personen die uiteindelijk eigenaar zijn van of zeggenschap hebben over de onderneming (niet enkel de juridische eigenaar op papier) en zij zijn essentieel voor het opsporen van verborgen eigendomsstructuren en mogelijke fraude of witwassen.

Opgelet

U moet de UBO('s) identificeren van elke onderneming waarmee u zaken doet.

Een persoon is een UBO indien hij of zij:

- 25% of meer van de aandelen of stemrechten van de onderneming bezit, of
- De onderneming op een andere manier controleert (bijvoorbeeld via een keten van vennootschappen)

Hoe UBO-informatie te vinden:

- Voor Belgische ondernemingen: raadpleeg het Belgische UBO-register op financien.belgium.be
- Voor buitenlandse ondernemingen: gebruik internationale databanken zoals Moody's (beschikbaar via KYCP), of vraag de informatie rechtstreeks aan uw tegenpartij

Indien de informatie die u vindt onvolledig of onduidelijk is, is het uw verantwoordelijkheid om uw tegenpartij om de juiste informatie te vragen en deze te verifiëren aan de hand van een betrouwbare bron.

3.2.3 Hoe AML-informatie verkrijgen en verifiëren

Om AML-informatie te verkrijgen, vraagt u uw tegenpartij om een Client Information Form in te vullen (voorbeeldformulieren zijn beschikbaar op de website van AWDC).

Indien de tegenpartij een beursgenoteerde onderneming is (een onderneming waarvan de aandelen genoteerd zijn en actief verhandeld worden op een gereguleerde openbare effectenbeurs) in de Europese Economische Ruimte, Australië, Hongkong of de Verenigde Staten, kan u deze ondernemingen op een vereenvoudigde manier identificeren, bijvoorbeeld via de website van de beursgenoteerde onderneming. De UBO's van een beursgenoteerde onderneming moeten niet worden geïdentificeerd.

3.2.4 Verifieer de informatie via een betrouwbare bron

Het verzamelen van informatie is niet voldoende — u moet ook nagaan of deze correct is. Dit is het verplichte verificatieproces.

Gebruik onafhankelijke en betrouwbare bronnen om te verifiëren wat uw tegenpartij u heeft meegedeeld:

- Kruispuntbank van Ondernemingen (KBO) — voor Belgische ondernemingen
- Belgisch UBO-register — voor UBO-informatie
- KYCP (Moody's / ORBIS) — voor internationale bedrijfsgegevens

Opgelet

Indien identiteitsdocumenten niet authentiek lijken, of bedrijfsgegevens niet overeenstemmen met officiële registers, mag u niet verdergaan.

Indien u een verschil vaststelt tussen de UBO-informatie in het Belgische UBO-register en de informatie die u hebt verzameld, moet u dit zonder uitstel melden aan het register (in ieder geval binnen 14 kalenderdagen na de vaststelling ervan).

3.3 Actualiseren en onderhouden van AML-gegevens

KYC-informatie moet gedurende de volledige zakelijke relatie accuraat blijven.

Werk uw informatie bij:

- Minstens elk jaar — voor tegenpartijen met een hoog risico
- Om de 2 tot 3 jaar — voor tegenpartijen met een laag risico
- Onmiddellijk — wanneer er zich een belangrijke wijziging voordoet (bijvoorbeeld nieuwe eigendomsstructuur, nieuwe UBO's, negatief nieuws)

Actualiseringsprocedure:

- Stuur het bestaande AML-dossier naar de tegenpartij.
- Vraag een schriftelijke bevestiging dat de informatie nog correct is.
- Werk de informatie indien nodig bij.

Opgelet

Uw AML-beleid moet duidelijk de frequentie en methode voor het actualiseren van informatie over tegenpartijen omschrijven. U moet transacties en gedrag voortdurend monitoren om ervoor te zorgen dat deze consistent blijven met het profiel van de tegenpartij.

Bewaar uw AML-gegevens:

AML-documenten moeten gedurende 10 jaar worden bewaard na het einde van de zakelijke relatie of na de datum van een occasionele transactie.

Opgelet

Tijdens deze periode moeten alle documenten op verzoek onmiddellijk beschikbaar zijn voor de FPS Economy (bijvoorbeeld tijdens een AML-controle).

Na 10 jaar bent u wettelijk verplicht om alle persoonsgegevens permanent te verwijderen of te anonimiseren — identificatiedocumenten, klantenformulieren, UBO-informatie en risicoanalyses — tenzij er een specifieke wettelijke reden bestaat om deze te bewaren (zoals een lopend onderzoek of een formeel verzoek van de autoriteiten).

Bij verwijdering moeten digitale bestanden permanent uit systemen en back-ups worden verwijderd; papieren documenten moeten worden vernietigd.

Houd een intern verwijderingsregister bij met de referentie van de tegenpartij, de datum van verwijdering en de gebruikte methode — maar zonder persoonsgegevens.

3.4 GDPR-overwegingen en non-compliance

AML-verplichtingen zijn gebaseerd op een wettelijke verplichting, wat betekent dat u persoonsgegevens mag verzamelen en verwerken zonder de toestemming van uw tegenpartij. Wanneer AML-regels en GDPR-regels tegenstrijdig lijken, hebben de AML-regels voorrang.

U moet tegenpartijen informeren dat hun gegevens worden verzameld. Uw tegenpartijen moeten geïnformeerd worden over:

- Het doel (AML-naleving)
- De bewaartermijn van de AML-informatie (10 jaar)
- Het feit dat deze informatie mogelijk gedeeld zal worden met de autoriteiten

Verzamel enkel wat noodzakelijk is. Tijdens de bewaartermijn kunnen tegenpartijen geen verwijdering eisen of bezwaar maken tegen de verwerking.

Weigering om informatie te verstrekken of identificatie is niet mogelijk

- Indien een tegenpartij weigert informatie te verstrekken of haar UBO's te identificeren: ga de relatie niet aan of zet deze niet verder, documenteer de weigering en beschouw dit als een hoogrisico-indicator. Indien u witwassen vermoedt (zelfs als u dit niet kan bewijzen), meld dit aan de CFI (zie hoofdstuk 5 – Melden van verdachte activiteiten).
- Indien identificatie eenvoudigweg niet mogelijk is ondanks redelijke inspanningen: hetzelfde gevolg — ga niet verder, documenteer de stappen die u hebt ondernomen en overweeg een melding aan de CFI.

3.5 Voortdurende waakzaamheid tijdens de zakelijke relatie

KYC eindigt niet wanneer een relatie begint. De frequentie van actualisering hangt af van het risicoprofiel van de tegenpartij (zie hoofdstuk 3.3 – Actualiseer en onderhoud uw AML-gegevens).

Gedurende de volledige relatie moet u:

- De informatie over de tegenpartij up-to-date houden (jaarlijks voor hoogrisicoprofielen; om de 2–3 jaar voor lage/middelhoge risicoprofielen — en onmiddellijk wanneer zich een belangrijke wijziging voordoet)
- Transacties monitoren om ervoor te zorgen dat ze consistent blijven met het profiel van de tegenpartij en de aard van de relatie
- Alert blijven voor hoogrisicosignalen: herhaalde verzoeken tot contante betalingen, negatieve berichtgeving in de media, veranderingen in eigendomsstructuren, ...

Indien een transactie ongebruikelijk lijkt — complex, uitzonderlijk groot of zonder duidelijke zakelijke reden — moet u deze onderzoeken, indien nodig inclusief de oorsprong van de fondsen, en uw analyse schriftelijk documenteren. Indien u geen bevredigende verklaring kan geven, moet u:

- Overwegen om de zakelijke relatie op te schorten of te beëindigen;
- Beoordelen of er een vermoeden bestaat van witwassen of terrorismefinanciering en, indien nodig,
- Een melding doen aan de CFI (zie hoofdstuk 5 – Melden van verdachte activiteiten)

Voer de KYC-controle uit:

- Weet wie uw tegenpartij is
- Weet wie eigenaar is van de tegenpartij en wie de UBO's zijn
- Verifieer de gegevens die u hebt verzameld
- Actualiseer de KYC-informatie op regelmatige basis
- Verwijder alle persoonsgegevens 10 jaar na het einde van de zakelijke relatie
- Kunt u uw tegenpartij niet identificeren? Ga de relatie niet aan / zet deze niet verder (en overweeg een melding aan de CFI)

Test uw kennis

(juiste antwoorden worden aan het einde van deze syllabus gegeven)

1. Een klant weigert een identiteitsdocument te verstrekken of de namen van de UBO's bekend te maken. Wat doet u?
 - a. De relatie voortzetten, de weigering documenteren en uw risicoanalyse aanpassen
 - b. De privacy van de klant respecteren en de relatie voortzetten
 - c. De relatie of transactie weigeren. Indien witwassen wordt vermoed, melden aan de CFI
 - d. De relatie voortzetten maar melden aan de federale gerechtelijke politie
2. Hoe lang moeten documenten worden bewaard nadat een zakelijke relatie is beëindigd?
3. Uw opzoeking levert geen informatie op over een tegenpartij. Wat doet u?
 - a. De tegenpartij als laag risico beschouwen
 - b. De tegenpartij als neutraal risico beschouwen en de zoekpoging documenteren
 - c. Niet verdergaan — u kunt niet voldoen aan uw identificatieverplichting
 - d. Verdergaan zonder bijkomende verificatie
4. Welke stappen moet een diamanthandelaar volgen om de UBO's van een buitenlandse onderneming te identificeren?
 - a. De onderneming of vertegenwoordiger vragen een verklaring te ondertekenen
 - b. Redelijke stappen ondernemen om informatie te verzamelen en te verifiëren (naam, adres, bestuurders, UBO's) en de documenten bewaren
 - c. Enkel informatie over bestuurders verzamelen indien het risico hoog is
 - d. Enkel naam en adres verzamelen — meer vragen zou in strijd zijn met de GDPR
5. KYC-gegevens moeten elk jaar worden bijgewerkt voor hoogrisicoklanten, en om de 2 tot 3 jaar voor andere klanten.
 - a. Juist
 - b. Onjuist
6. Welk minimumpercentage van eigendom kwalificeert iemand als een UBO in België?

Hoofdstuk 4: Risicoanalyse en hoogrisicosituaties

Wat leer ik in dit hoofdstuk?

4.1 Wat is een risicoanalyse en waarom moet u deze uitvoeren?

4.2 Wanneer moet u een risicoanalyse uitvoeren?

4.3 Welke informatie heeft u nodig om een correcte risicoanalyse uit te voeren?

4.4 Risicocategorieën waarmee rekening moet worden gehouden

4.5 Risicoclassificatie: laag, middel en hoog

4.6 Resultaat van uw risicoanalyse: aanvaarden of weigeren?

Dit hoofdstuk is opgesplitst in twee delen:

Deel A: Theorie. Wat is een risicoanalyse, hoe en wanneer moet u deze uitvoeren en hoe classificeert u risico's?

Deel B: Hoogrisicosituaties in de praktijk: hoe past u de theorie toe in de meest voorkomende hoogrisicoscenario's waarmee u geconfronteerd kan worden.

DEEL 1: THEORIE

4.1 Wat is een risicoanalyse en waarom moet u deze uitvoeren?

Een risicoanalyse is een essentiële stap in het voorkomen van witwassen en terrorismefinanciering.

Voordat u zaken doet, moet u het risico beoordelen van het samenwerken met een tegenpartij (klant of leverancier) **en dit moet je op verschillende belangrijke momenten tijdens de zakelijke relatie herhalen.**

U stelt uzelf één fundamentele vraag: Hoe risicovol is het om zaken te doen met deze persoon of onderneming?

Het antwoord op deze vraag zal duidelijk zijn nadat u een risicoanalyse hebt uitgevoerd.

Een risicoanalyse volgt een risicogebaseerde aanpak. Dit betekent dat niet elke tegenpartij aan hetzelfde niveau van controles wordt onderworpen. In plaats daarvan past u uw controlemaatregelen aan het risiconiveau aan:

- Tegenpartijen met een laag risico vereisen standaardcontroles
- Tegenpartijen met een hoog risico vereisen bijkomende controles (Enhanced Due Diligence of EDD genoemd)

Het doel van een risicoanalyse is om:

- Te weten en te verifiëren met wie u zaken doet (uw tegenpartij identificeren): KYC (zie hoofdstuk 3 – Know Your Counterparty)
- Te begrijpen waar hun geld vandaan komt
- Ongebruikelijke of verdachte situaties te detecteren
- Te beslissen of u een zakelijke relatie veilig kan aangaan of voortzetten

Het herkennen van hoogrisicosituaties is een essentieel onderdeel van dit proces. Dit zijn situaties waarbij het risico op witwassen of fraude hoger is en waarbij bijkomende controles vereist zijn (ook Enhanced Due Diligence (EDD) genoemd).

4.2

Wanneer moet u een risicoanalyse uitvoeren?

4.2.1 Risicoanalyse van uw eigen onderneming

Voordat er zaken worden gedaan, moet u een algemene analyse maken van de AML-risico's binnen uw eigen onderneming.

Door uw eigen risico's te begrijpen, kan u de juiste controlemaatregelen invoeren en vermijden dat u onbewust betrokken raakt bij witwassen of inbreuken op sancties.

Gebruik de risicoscorekaart in Bijlage A van deze syllabus om het AML-risicoprofiel van uw onderneming manueel te beoordelen, of gebruik het KYCP-portaal om de beoordeling digitaal uit te voeren.

4.2.2 Risicoanalyse van uw tegenpartij

Een risicoanalyse van uw tegenpartij moet worden uitgevoerd op verschillende belangrijke momenten **voor en tijdens** uw zakelijke activiteiten. Deze is niet beperkt tot de start van een relatie, maar geldt gedurende de volledige looptijd van uw interactie met een tegenpartij.

Voordat u een zakelijke relatie aangaat

- Is het veilig en gepast om met deze persoon of onderneming samen te werken?

Vóór een occasionele transactie

- Zelfs als er geen doorlopende relatie bestaat, moet u nog steeds de risico's beoordelen die verbonden zijn aan de transactie en de betrokken tegenpartij.

Wanneer er iets belangrijks verandert (in de relatie)

- Zoals nieuwe uiteindelijke begunstigden (UBO's), nieuwe eigenaars, wijzigingen in de bedrijfsactiviteiten van de klant of andere relevante ontwikkelingen die een impact kunnen hebben op het risicoprofiel, moet u het risico opnieuw beoordelen.

Wanneer een transactie ongebruikelijk lijkt

- Transacties die uitzonderlijk groot of complex zijn, of geen duidelijk economisch doel hebben.

Als onderdeel van een regelmatige periodieke herziening (voortdurende monitoring)

- Klantendossiers en risicoprofielen moeten gedurende de volledige relatie worden herzien en up-to-date gehouden. De frequentie van de herziening hangt af van het risicoprofiel (hoog, middel, laag) van de tegenpartij.

Opgelet

Een risicoanalyse is nooit een eenmalige oefening. U moet de analyse opnieuw uitvoeren telkens wanneer de omstandigheden veranderen.

4.3

Welke informatie heeft u nodig om een correcte risicoanalyse uit te voeren?

Om het risico correct te beoordelen, moet u vijf zaken begrijpen over uw tegenpartij en de transactie:

- **Begrijp het doel van de zakelijke relatie of transactie**

Dit betekent dat u nagaat waarom de klant zaken met u wil doen. Wat willen zij kopen of verkopen?

Voorbeeld

Een juwelier wil geslepen diamanten kopen voor wederverkoop in zijn winkel → logisch.

Een bouwbedrijf wil diamanten van hoge waarde kopen → ongebruikelijk en vereist verder onderzoek.

- **Begrijp wat de omvang van de verwachte zakelijke relatie zal zijn**

Dit betekent dat u weet wat de verwachte waarde van de transacties is, hoe frequent transacties zullen plaatsvinden en wat het verwachte volume aan diamanten is dat verhandeld zal worden.

Voorbeeld

Een nieuwe klant wil onmiddellijk voor €2 miljoen aan diamanten kopen in één transactie, zonder zichtbare staat van dienst → hoger risico.

Een langetermijnklant die kleinere, regelmatige partijen aankoopt → lager risico.

- **Bepaal de oorsprong van de fondsen**

U begrijpt waar het geld dat voor de transactie wordt gebruikt vandaan komt. Is de oorsprong ervan legitiem en kan u dit verifiëren?

Voorbeeld

De betaling komt van een gekende bedrijfsrekening die overeenstemt met de bedrijfsactiviteiten van de klant → weinig bezorgdheid.

De betaling komt van een privérekening of een niet-gerelateerde derde partij → alarmsignaal.

- **Bepaal de bestemming van de fondsen**

U weet waar het geld of de diamanten naartoe gaan, en of deze bestemming logisch en legitiem is binnen de context van de transactie.

Voorbeeld

Een diamantgroothandelaar die ruwe diamanten aankoopt → consistent.

Een individu zonder duidelijke bedrijfsactiviteit dat grote volumes diamanten verhandelt → ongebruikelijk en hoger risico.

- **Beoordeel de bedrijfsactiviteit of het beroep van de tegenpartij**

U moet nagaan of de activiteiten van de tegenpartij overeenstemmen met de beoogde transactie of relatie.

Om te begrijpen welke soorten risico's verbonden kunnen zijn aan uw tegenpartij, kan u gebruikmaken van de risicoscorekaart in Bijlage B of gebruikmaken van de GRID-screeningtool die beschikbaar is via het KYCP-platform (zie hoofdstuk 7 – AML-templates, tools en handleidingen).

Opgelet

Het resultaat van de risicoscreening zal een impact hebben op de uiteindelijke beslissing om de tegenpartij al dan niet te onboarden. Zowel de risicoscorekaart als de resultaten van de risicoscreening via KYCP ondersteunen de handelaar bij het nemen van deze beslissing (zie hieronder, hoofdstuk 4.7 – Resultaat: Aanvaarden of Weigeren?).

4.4 Risicocategorieën waarmee rekening moet worden gehouden

Er bestaat geen officiële of exhaustieve lijst van risico's waarmee rekening moet worden gehouden bij het uitvoeren van een risicoanalyse. U moet altijd uw eigen professionele beoordeling toepassen, gebaseerd op de specifieke situatie en de beschikbare informatie.

Er zijn echter vier risicocategorieën die u kunnen helpen om uw analyse te structureren. Indien één of meerdere van onderstaande vragen met “ja” kunnen worden beantwoord, kan dit wijzen op een hoogrisicosituatie waarvoor bijkomende controles vereist zijn.

1. Risico van de tegenpartij – gerelateerd aan de kenmerken, achtergrond en het gedrag van uw tegenpartij:

- Is uw tegenpartij een PEP (Politically Exposed Person)?
- Wordt de tegenpartij gelinkt aan negatieve berichtgeving of media?
- Kan of wil de tegenpartij het doel van de transactie of zakelijke relatie niet uitleggen?
- Heeft de tegenpartij in het verleden faillissementen of financiële moeilijkheden gekend?
- Heeft de onderneming een complexe of onduidelijke eigendomsstructuur (UBO's)?

2. Geografisch risico – gerelateerd aan het land of de regio waarmee uw tegenpartij of transactie verbonden is:

- Is de tegenpartij of transactie gelinkt aan een hoogrisicoland
- Is de tegenpartij of transactie gelinkt aan een gesanctioneerd land of rechtsgebied?

3. Transactierisico – gerelateerd aan de aard en kenmerken van de transactie zelf:

- Is de transactie uitzonderlijk groot of stemt deze niet overeen met het profiel of de bedrijfsactiviteiten van de tegenpartij?
- Wil de tegenpartij in contanten betalen?
- Wil de tegenpartij via een derde partij betalen?
- Dringt de tegenpartij aan op ongebruikelijke of complexe betaalmethoden?

4. Product-/sectorrisico – gerelateerd aan de inherente kenmerken van de verhandelde goederen en de aard van de diamantsector:

- Heeft de transactie betrekking op diamanten van hoge waarde?
- Zijn de goederen gemakkelijk transporteerbaar? Diamanten zijn klein en eenvoudig te verplaatsen, waardoor ze kwetsbaarder zijn voor smokkel en illegale handel.
- Ontbreekt er een duidelijke economische logica in de transactie of handelsstructuur?

Opgelet

Deze vier categorieën weerspiegelen de risicoscorekaart in Bijlage B. Doorloop elke categorie systematisch voor elke nieuwe tegenpartij en telkens wanneer uw beoordeling moet worden geactualiseerd.

4.5

Risicoclassificatie: laag, medium en hoog

Nadat u alle relevante informatie hebt verzameld en mogelijke risicofactoren hebt geïdentificeerd, kan u een risiconiveau toekennen aan uw tegenpartij. Dit wordt risicoclassificatie genoemd.

In de praktijk worden tegenpartijen doorgaans geclassificeerd als laag, middel of hoog risico.

Risicolevel	Kenmerken	Due Diligence Vereisten
 LAAG	Duidelijke identiteit, eenvoudige structuur, geen alarmsignalen, consistente transacties	Standaard due diligence: basisidentificatie, verificatie, routinematige monitoring
 MEDIUM	Enkele risicofactoren aanwezig maar verklaarbaar; licht complexe structuur	Vereenvoudigde due diligence: bijkomende vragen, verhoogde aandacht, meer monitoring
 HOOG	Eén of meerdere significante risico-indicatoren, of een gebrek aan transparantie	Enhanced Due Diligence (EDD): bijkomende informatie, oorsprong van de fondsen, goedkeuring door het management, verhoogde monitoring

Risiconiveau: laag risico

Een tegenpartij wordt beschouwd als laag risico wanneer er geen significante risico-indicatoren aanwezig zijn en de situatie duidelijk, transparant en consistent is.

Dit betekent:

- De identiteit en eigendomsstructuur zijn eenvoudig en gemakkelijk te verifiëren
- De bedrijfsactiviteit is duidelijk en logisch
- De transactie past binnen het profiel van de tegenpartij
- Er zijn geen links met hoogrisicolanden, PEP's of negatieve media

Voor klanten met een laag risico past u standaard due diligence toe. Dit omvat basisidentificatie, verificatie en routinematige monitoring.

Risiconiveau: middel risico

Een tegenpartij wordt beschouwd als middel risico wanneer bepaalde risicofactoren aanwezig zijn, maar deze redelijk kunnen worden verklaard en niet onmiddellijk aanleiding geven tot verdenking.

Dit kan onder meer omvatten:

- Een iets complexere ondernemingsstructuur
- Transacties die groter of minder gebruikelijk zijn, maar nog steeds kunnen worden gerechtvaardigd
- Beperkte banden met jurisdicties of sectoren met een hoger risico

Voor tegenpartijen met een middel risico moet u vereenvoudigde due diligence toepassen: stel bijkomende vragen, verifieer bepaalde elementen grondiger en monitor transacties nauwkeuriger.

Risiconiveau: hoog risico

Een tegenpartij wordt beschouwd als hoog risico wanneer één of meerdere significante risico-indicatoren aanwezig zijn, of wanneer er een gebrek aan transparantie is.

Voorbeelden:

- Politically Exposed Persons (PEP's)
- Banden met hoogrisico- of gesanctioneerde landen
- Gebruik van contanten, betalingen via derden of ongebruikelijke transactiestructuren
- Complexe of onduidelijke eigendomsstructuren
- Negatieve berichtgeving in de media of reputatierisico's

Voor tegenpartijen met een hoog risico moet u Enhanced Due Diligence (EDD) toepassen. Dit omvat:

- Het verzamelen van bijkomende informatie en documentatie
- Het verifiëren van de oorsprong van de fondsen en, indien relevant, de oorsprong van het vermogen
- Het verkrijgen van interne goedkeuring voordat de transactie of zakelijke relatie wordt aangegaan
- Het toepassen van verhoogde en voortdurende monitoring

Indien de risico's niet voldoende kunnen worden begrepen of beperkt, moet u de zakelijke relatie of transactie weigeren.

4.6

Resultaat van uw risicoanalyse: aanvaarden of weigeren?

Na het uitvoeren van een risicoanalyse moet u beslissen hoe u verdergaat met de tegenpartij. De beslissing hangt af van het vastgestelde risiconiveau en van de maatregelen die u kan nemen om dit risico te beperken.

De drie mogelijke beslissingen zijn:

Beslissing	Wanneer	Wat te doe
✓ ACCEPTEER	Het risico is laag of beheersbaar.	Ga verder met standaardmonitoring en reguliere due diligence.
⚠ ACCEPTEER MET VOORWAARDEN	Het risico is middelmatig of kan worden beperkt.	Pas Enhanced Due Diligence (EDD) toe; verkrijg goedkeuring van het management voordat u verdergaat.
⊘ WEIGER	Het risico is te hoog of alarmsignalen kunnen niet worden verklaard.	Ga niet verder. Meld aan de CFI indien u witwassen vermoedt.

Opgelet

- U moet uw beslissing om een tegenpartij te aanvaarden, onder voorwaarden te aanvaarden of te weigeren kunnen motiveren.
- Elke beslissing moet duidelijk worden gedocumenteerd, inclusief de beoordeelde informatie, de in aanmerking genomen risicofactoren en de motivering achter uw keuze.

AWDC biedt een kant-en-klare template voor KYC- en risicoanalyseconclusies aan om u te helpen uw beslissing op een consistente manier te documenteren:



4.6.1 Documentatie en archivering

Elke risicoanalyse en gerelateerde beslissing moet worden geregistreerd zodat deze kan worden gecontroleerd en geaudit. Bewaar een overzicht van:

- Het toegekende risiconiveau — laag, middel of hoog
- Belangrijkste bevindingen — informatie en observaties waarop uw beoordeling is gebaseerd
- Beslissing en motivering — wat u hebt beslist (aanvaarding, aanvaarding onder voorwaarden of weigering) en waarom
- Ondersteunende documenten — kopieën van identiteitsdocumenten, contracten, e-mails, screeningresultaten

Opgelet

Alle documenten moeten georganiseerd en raadpleegbaar zijn. Zorg ervoor dat deze informatie op verzoek beschikbaar is, bijvoorbeeld tijdens AML-controles.

DEEL 2: HOOGRISICOSITUATIES IN DE PRAKTIJK EN HOE HIEROP TE REAGEREN

De onderstaande secties behandelen de vijf hoogrisicosituaties waarmee u als diamanthandelaar het meest waarschijnlijk geconfronteerd zal worden. Elke sectie volgt dezelfde structuur:

- Wat het is (de theorie)
- Waarom het belangrijk is voor AML
- Wat u moet doen
- Een praktisch voorbeeld

4.6.2 Politically Exposed Persons (PEP's)

Wat is een PEP?

- Een Politically Exposed Person (PEP) is iemand die een prominente publieke functie bekleedt — of heeft bekleed. Deze categorie omvat:
- Staatshoofden of regeringsleiders, ministers en hooggeplaatste politici
- Rechters van hoge rechtbanken en hoge militaire functionarissen
- Leidinggevendenden van staatsbedrijven
- Directe familieleden (echtgenoot/echtgenote, kinderen, ouders)
- Nauwe geassocieerden (gekende zakenpartners, nauwe connecties)

Opgelet

Een persoon blijft een PEP tijdens de uitoefening van zijn of haar functie en gedurende minstens 12 maanden nadat de functie werd beëindigd — en soms langer, afhankelijk van de algemene risicoanalyse.

Waarom is de PEP-status belangrijk voor AML?

PEP's worden beschouwd als een hoger risico omdat:

- Zij mogelijk toegang hebben tot publieke middelen
- Zij meer blootgesteld kunnen zijn aan corruptie of omkoping
- Er een hoger risico bestaat op witwassen gelinkt aan machtsmisbruik

Opgelet

PEP zijn betekent NIET dat de persoon iets illegaals doet. Het betekent enkel dat extra voorzichtigheid vereist is. U kan nog steeds zaken doen met een PEP — maar enkel nadat u Enhanced Due Diligence (EDD) hebt uitgevoerd.

Wat moet u doen wanneer u een PEP identificeert?

- Verzamel bijkomende informatie, zoals de oorsprong van het vermogen (hoe de persoon rijkdom heeft vergaard), de oorsprong van de fondsen (waar het geld dat voor de transactie wordt gebruikt vandaan komt) en het doel van de zakelijke relatie
- Voer een diepgaandere verificatie uit: gebruik betrouwbare en onafhankelijke bronnen, controleer media en publieke informatie, en screen tegen sanctie- en watchlists
- Verkrijg goedkeuring van het senior management voordat u zaken doet met een PEP. Een relatie met een PEP kan niet enkel op operationeel niveau worden goedgekeurd
- Verhoog de monitoring: voer frequentere controles van de relatie uit en monitor de transacties nauwkeuriger

Controleer de PEP-status via KYCP (dat toegang geeft tot GRID), Google, officiële overheidswebsites en openbare registers.

- U kan controleren of een tegenpartij een PEP is via het KYCP-platform (dat toegang biedt tot GRID, een uitgebreide screening- en monitoringdatabase), Google-opzoeken, officiële overheidswebsites, openbare registers, ...
- PEP-status is een risico-indicator, geen verbod. U kan nog steeds zaken doen met een PEP, maar enkel indien u: de oorsprong van de fondsen volledig begrijpt, enhanced checks toepast en de relatie nauwgezet monitort.

Voorbeeld

U wordt gecontacteerd door een nieuwe klant die een gepensioneerd minister is uit een Afrikaans land. Hij wil een partij geslepen diamanten van hoge waarde aankopen.

Stap 1 — Identificeren: Tijdens de KYC ontdekt u zijn voormalige ministerfunctie. Hij is een PEP.

Stap 2 — Verzamel bijkomende informatie: Vraag waar het geld vandaan komt (oorsprong van de fondsen) en hoe hij zijn vermogen heeft opgebouwd (oorsprong van het vermogen).

Stap 3 — Verifiëren: Controleer zijn informatie aan de hand van GRID (voor sanctie- en PEP-databanken), publieke media en officiële registers.

Stap 4 — Goedkeuring: Voordat u verdergaat, moet u de zaak escaleren naar het senior management voor formele goedkeuring.

Stap 5 — Monitoring: Indien de relatie wordt aanvaard, moet u deze frequenter monitoren dan een standaardtegenpartij.

Indien u de oorsprong van de fondsen of het vermogen niet op een bevredigende manier kan verifiëren, moet u de relatie weigeren en — indien u witwassen vermoedt — een melding doen aan de CFI.

4.6.3 Zaken doen met een tegenpartij gevestigd in een ‘hoogrisicoland’

Een hoogrisicoland is een land met een verhoogd risico op witwassen of terrorismefinanciering, bijvoorbeeld door zwakke controlesystemen of hoge niveaus van corruptie.

Tegenpartijen die gelinkt zijn aan dergelijke landen worden automatisch beschouwd als een hoger risico. Dit betekent dat u Enhanced Due Diligence (EDD) moet toepassen voordat u de zakelijke relatie aangaat of voortzet.

Er bestaan verschillende landenlijsten (**black & grey list**), gepubliceerd door de FATF, die strategische tekortkomingen in AML-kaders op verschillende niveaus identificeren. Zaken doen met ondernemingen gevestigd in deze landen is ofwel verboden, of vereist Enhanced Due Diligence (EDD).

Black list

Landen op de hoogrisico- (“zwarte”) lijst zijn onder meer:

- Myanmar
- Democratische Volksrepubliek Korea (DPRK)
- Iran

De FATF roept op tot de toepassing van verscherpte cliëntenonderzoeksmaatregelen (Enhanced Due Diligence, EDD) en, waar nodig, het invoeren van tegenmaatregelen. Deze maatregelen kunnen van land tot land verschillen. De Belgische Antiwitwaswet definieert "hoogrisico derde landen" als landen die onder meer door de Financial Action Task Force (FATF) als hoogrisico zijn geïdentificeerd. Ten aanzien van hoogrisico derde landen moeten steeds verscherpte cliëntenonderzoeksmaatregelen (EDD) worden toegepast, waaronder:

- Het inwinnen van bijkomende informatie over de cliënt en de uiteindelijke begunstigde(n) (UBO's);
- Het inwinnen van bijkomende informatie over de beoogde aard van de zakelijke relatie;
- Het inwinnen van informatie over de herkomst van de middelen en het vermogen van de cliënt en de uiteindelijke begunstigde(n);
- Het inwinnen van informatie over de redenen voor de beoogde of uitgevoerde transacties;
- Het verkrijgen van goedkeuring van het hoger leidinggevend personeel voorafgaand aan het aangaan of voortzetten van de zakelijke relatie;
- Het uitvoeren van verscherpte monitoring van de zakelijke relatie, door het aantal en de frequentie van controles te verhogen en door transactiepatronen te identificeren die verdere aandacht vereisen;
- Waar toepasselijk, ervoor zorgen dat de eerste betaling gebeurt via een rekening op naam van de cliënt bij een kredietinstelling die cliëntenonderzoeksnormen toepast die minstens gelijkwaardig zijn aan diegene vastgelegd in deze wet.

De grijze lijst

Landen op deze lijst worden door de FATF beschouwd als onderworpen aan verscherpt toezicht. De FATF beveelt geen tegenmaatregelen aan tegen landen op de grijze lijst, en verbiedt evenmin zakelijke relaties met deze landen. In plaats daarvan worden deze landen verplicht om hun AML/CFT-controlekaders te verbeteren en over hun vooruitgang te rapporteren aan de FATF.

De Belgische Antiwitwaswet maakt geen onderscheid tussen de zwarte lijst en de grijze lijst van de FATF. De wet verwijst in plaats daarvan naar landen met een verhoogd geografisch risico. Op basis van de classificaties van de FATF betreft dit voornamelijk de landen op de zwarte lijst. Niettemin is het aan te raden om verscherpte cliëntenonderzoeksmaatregelen (EDD) toe te passen bij tegenpartijen of transacties die verbonden zijn aan landen op de grijze lijst.

Opgelet

Zaken doen met deze landen is verboden OF onderworpen aan de strengste EDD-controles.

U kan de officiële lijsten raadplegen die gepubliceerd worden door de European Commission en de Financial Action Task Force. Deze lijsten worden regelmatig geactualiseerd en moeten telkens opnieuw worden gecontroleerd.



Wat moet u doen wanneer u zaken doet met een tegenpartij uit een hoogrisicoland?

- Verzamel bijkomende identificatie-informatie van uw tegenpartij, inclusief geverifieerde identiteitsdocumenten en gegevens van de uiteindelijke begunstigten (UBO's) — standaardcontrole voor elke tegenpartij
- Verifieer de oorsprong van de fondsen (en, indien nodig, de oorsprong van het vermogen) om ervoor te zorgen dat het geld legitiem is
- Controleer de betrokken bank om te bevestigen dat deze betrouwbaar is en correcte AML-controles toepast
- Begrijp het doel van de transactie en zorg ervoor dat deze economisch logisch is
- Verkrijg interne goedkeuring (bv. van uw management of AML officer) voordat u deze zakelijke relatie aangaat
- Pas verhoogde monitoring toe tijdens de zakelijke relatie

Opgelet

Indien de risico's niet voldoende kunnen worden beperkt, moet u de transactie of de zakelijke relatie weigeren.

Documenteer altijd uw beoordeling, de genomen maatregelen en uw beslissing. Deze informatie moet op verzoek beschikbaar zijn, bijvoorbeeld tijdens een AML-controle.

Praktisch voorbeeld

Een leverancier contacteert u met het aanbod van een partij ruwe diamanten. Zijn onderneming is geregistreerd in een land dat momenteel op de FATF-grijze lijst staat.

Stap 1 — Geografisch risico identificeren: Het land van oorsprong alleen al plaatst deze situatie in een hogere risicocategorie. U kan geen standaard due diligence toepassen.

Stap 2 — Enhanced KYC: Vraag volledige UBO-gegevens, geverifieerde identiteitsdocumenten en gedetailleerde informatie over hoe de onderneming opereert.

Stap 3 — Oorsprong van de fondsen: Vraag bewijs van hoe de leverancier deze diamanten heeft verkregen en waar de betalingsmiddelen vandaan komen.

Stap 4 — Bankcontrole: Verifieer dat de bank die de leverancier gebruikt betrouwbaar is en over adequate AML-controles beschikt.

Stap 5 — Goedkeuring door management: Escaleer de zaak voor formele goedkeuring voordat u de relatie aangaat.

Stap 6 — Voortdurende monitoring: Indien u verdergaat, moet u de relatie frequenter evalueren dan bij een standaardtegenpartij.

4.6.4 Zaken doen met een tegenpartij of transactie gelinkt aan een gesanctioneerd land of rechtsgebied

Wat zijn sancties?

Sancties zijn wettelijke beperkingen opgelegd door overheden of internationale instanties die zaken doen met bepaalde landen, entiteiten of individuen beperken of verbieden. In tegenstelling tot de FATF-grijze lijst (waarvoor EDD vereist is), kunnen sancties een transactie volledig verbieden.

De FPS Finance is verantwoordelijk voor het toezicht op en de naleving van de internationale financiële sancties die door de EU worden opgelegd.

Een belangrijk voorbeeld zijn de EU-sancties tegen Rusland, naar aanleiding van de oorlog van Rusland tegen Oekraïne:

Sinds 1 januari 2024 vallen Russische diamanten onder de EU-sancties, waardoor het wettelijk verboden is om diamanten van Russische oorsprong in te voeren of uit te voeren. Deze maatregel is van toepassing op:

- Alle niet-industriële natuurlijke diamanten (ruw en geslepen) van 0,5 karaat of groter;
- Alle niet-industriële synthetische diamanten van 0,5 karaat of groter;

Het verbod geldt ongeacht van waar de diamanten worden verzonden. Het omleiden van goederen via een derde land (zoals Dubai) maakt een anders verboden transactie NIET legaal.

Opgelet

Indien u diamanten wilt invoeren of uitvoeren die vermoedelijk van Russische oorsprong zijn en u geen correcte documentatie kan voorleggen om het tegendeel te bewijzen, zullen deze diamanten worden beschouwd als verboden goederen en zal de douane een onderzoek opstarten.

Industriële diamanten vallen niet onder deze sancties.

De verschillende fasen van de EU-sancties tegen Rusland zijn:

- De eerste fase: startte op 1 januari 2024: Dit was het moment waarop de invoer van diamanten van Russische oorsprong of diamanten die rechtstreeks uit Rusland komen, illegaal werd (= direct verbod).
- De tweede fase: startte op 1 maart 2024: Vanaf dit moment werd ook de indirecte invoer van Russische diamanten illegaal (bijvoorbeeld wanneer ze eerst geslepen werden in een derde land zoals India). Tijdens deze fase, ook wel de 'Sunrise Period' genoemd, is documentair bewijs vereist om de oorsprong van diamanten aan te tonen (en dat het geen Russische diamanten betreft) bij invoer in België via de Diamond Office. Alle diamanten die tijdens deze periode (1 maart tot 1 september 2024) binnen het toepassingsgebied vallen, zijn natuurlijke, niet-industriële, ruwe en geslepen diamanten van 1 karaat of groter.
- De derde fase: van kracht sinds 1 september 2024: Vanaf dit moment worden synthetische diamanten toegevoegd aan het toepassingsgebied, waardoor dit voortaan natuurlijke en synthetische, niet-industriële, ruwe en geslepen diamanten van 0,5 karaat of groter omvat. Vanaf dit moment kunnen Belgische Geregistreerde Diamanthandelaars ook hun bestaande voorraad regulariseren, bestaande uit diamanten van Russische of onbekende oorsprong. Dit wordt het zogenaamde 'Grandfathering Principle' genoemd.
- De vierde fase: startte op 1 maart 2025: Er werd een nieuwe vereiste toegevoegd voor de invoer van ruwe diamanten met gemengde oorsprong, in het kader van het Zestiende Sanctiepakket tegen Rusland. Bij de invoer van ruwe diamanten in de EU die binnen het toepassingsgebied vallen (alle natuurlijke, niet-industriële, ruwe diamanten van 0,5 karaat of groter), moeten KP-certificaten voortaan alle landen van oorsprong vermelden. Gemengde oorsprong wordt niet langer aanvaard op het KP-certificaat.
- Vijfde fase: afgerond tegen 1 januari 2026: Vanaf 1 januari 2026 moeten handelaars die geslepen diamanten invoeren die binnen het toepassingsgebied vallen*, een Due Diligence-verklaring over de oorsprong van de diamant toevoegen aan hun douaneaangifte.

*natuurlijke geslepen diamanten van 0,5 karaat of groter

Het is ook belangrijk op te merken dat de Russische diamantproducent Alrosa op de Europese sanctielijst staat. Bijgevolg mag u geen diamanten aankopen van Alrosa, zelfs niet wanneer het om diamanten kleiner dan 0,5 karaat gaat.

Voor gedetailleerde richtlijnen over de EU-sancties tegen Rusland en welke documentatie vereist is bij de invoer en uitvoer van diamanten, zie:



Praktisch voorbeeld

Een klant biedt u geslepen diamanten aan (elk groter dan 0,5 ct) die vanuit Dubai werden verzonden. De bijhorende documenten zijn vaag over het oorspronkelijke land van ontginning.

Stap 1 — Identificeer de onduidelijkheid: Dubai is een belangrijke transit-hub. Verzending vanuit Dubai bewijst niet dat de diamanten geen Russische oorsprong hebben.

Stap 2 — Vraag documentatie op: Vraag de volledige chain of custody op — het land van ontginning, het Kimberley Process-certificaat en alle invoer-/uitvoerdocumenten uit het land van oorsprong.

Stap 3 — Beoordelen: Indien de klant geen documentatie kan of wil voorleggen die bewijst dat de diamanten geen Russische oorsprong hebben, moet u de goederen beschouwen als mogelijk verboden.

Stap 4 — Beslissing: Weiger de transactie.

Indien u vermoedt dat iemand opzettelijk sancties probeert te omzeilen, moet u dit melden aan de CFI.

4.6.5 Transacties met een Amerikaanse link (US Nexus)

Een transactie kan een Amerikaanse link ("US nexus") hebben wanneer er een verband bestaat met de Verenigde Staten, zoals een Amerikaanse persoon, een Amerikaans bedrijf, een betaling in Amerikaanse dollar (USD), een Amerikaanse financiële instelling, of goederen bestemd voor de Amerikaanse markt. Zelfs wanneer een diamanthandelaar niet gevestigd is in de Verenigde Staten, kunnen Amerikaanse regelgeving en sancties nog steeds relevant zijn wanneer een dergelijke link bestaat.

Transacties met een Amerikaanse link moeten worden behandeld als hoger risico en vereisen verscherpte cliëntenonderzoeksmatregelen (Enhanced Due Diligence, EDD). Dit omvat het verifiëren van de identiteit van alle betrokken partijen, het screenen van tegenpartijen tegen de toepasselijke sanctielijsten, het begrijpen van de herkomst en bestemming van de fondsen, en het waarborgen dat de transactie geen verboden personen, entiteiten of goederen betreft. Bijzondere aandacht moet worden besteed aan USD-betalingen, aangezien deze vaak worden verwerkt via het Amerikaanse financiële systeem en daardoor onderworpen kunnen zijn aan bijkomende controle.

👉 Documenteer steeds de vastgestelde Amerikaanse link, de uitgevoerde controles, en de motivering voor het al dan niet voortzetten van de transactie

4.6.6 Een tegenpartij hebben die via een derde partij wil betalen

Een betaling via een derde partij doet zich voor wanneer een andere persoon of onderneming dan de gefactureerde tegenpartij de betaling uitvoert. Als algemene regel geldt: de partij die wordt gefactureerd, moet ook de partij zijn die betaalt.

Betalingen via derden worden beschouwd als een hoogrisicosituatie omdat ze kunnen worden gebruikt om de werkelijke oorsprong van de fondsen of de identiteit van de betrokken partijen te verbergen.

U mag een betaling via een derde partij enkel aanvaarden indien:

- De transactie volledig transparant is: u begrijpt duidelijk wie betaalt, namens wie en om welke reden
- Er een schriftelijke overeenkomst bestaat tussen alle betrokken partijen: deze overeenkomst moet de relatie uitleggen en de betalingsstructuur rechtvaardigen
- U uw uitdrukkelijke toestemming hebt gegeven: u moet de situatie beoordelen en akkoord gaan met de regeling voordat de betaling wordt uitgevoerd

In de praktijk beschouwen veel banken betalingen via derden als een hoog risico en kunnen zij weigeren deze te verwerken.

Opgelet

Indien u vermoedt dat een betaling via een derde partij gelinkt is aan illegale activiteiten, moet u de transactie weigeren.

Documenteer altijd de reden waarom u een betaling via een derde partij aanvaardt of weigert. Voor richtlijnen kan u verwijzen naar de AWDC Best Practice Guide, die een template voor een driepartijenovereenkomst bevat.



Praktisch voorbeeld

U factureert een diamantkoper in Hongkong voor een partij geslepen diamanten. Kort voordat de betaling verschuldigd is, ontvangt u een bericht dat de betaling zal gebeuren door een onderneming in een ander land — een onderneming waarvan u nog nooit hebt gehoord en die nergens in uw KYC-dossier vermeld staat.

Stap 1 — Stop: Aanvaard de betaling niet totdat u begrijpt wie betaalt en waarom.

Stap 2 — Vraag een schriftelijke uitleg: Vraag een schriftelijke overeenkomst, ondertekend door alle drie de partijen, waarin de relatie en de reden voor de betaling via een derde partij worden uitgelegd.

Stap 3 — Verifieer de derde partij: Pas KYC en een risicoanalyse toe op de derde partij — deze maakt nu deel uit van uw transactie.

Stap 4 — Beoordelen: Indien de uitleg bevredigend is en de derde partij kan worden geverifieerd, kan u verdergaan — mits gedocumenteerde toestemming.

Stap 5 — Alarmsignaal: Indien de koper de regeling niet kan of wil uitleggen, weiger dan de betaling en beoordeel of een melding aan de CFI vereist is.

4.6.7 Een tegenpartij hebben die in contanten wil betalen

Waarom zijn contante betalingen een hoogrisicosituatie?

Contante betalingen zijn van nature moeilijk traceerbaar. In tegenstelling tot bankoverschrijvingen laten cashbetalingen weinig of geen audit trail achter, waardoor ze aantrekkelijker zijn voor criminelen die de oorsprong van fondsen willen verbergen.

Om deze reden worden contante betalingen — vooral grote bedragen — beschouwd als een hoogrisico-indicator waarvoor Enhanced Due Diligence vereist is.

Limieten voor contante betalingen die u moet kennen

Scope	Limiet	Wat dit betekent
België	€3,000 per transactie	Dit is een strikte wettelijke maximumgrens. Betalingen opsplitsen in kleinere bedragen om onder deze limiet te blijven (ook wel “structuring” genoemd) is eveneens verboden.
EU grens (binnen/buiten)	€10,000 aangiftedrempel	Iedereen die een EU-grens overschrijdt met €10.000 of meer in contanten moet dit aangeven bij de douane.
Buiten België	Lokale regels van toepassing	U moet altijd de regels inzake contante betalingen naleven van het land waar de transactie plaatsvindt.

Opgelet

Indien een tegenpartij erop aandringt om een bedrag van meer dan €3.000 in contanten te betalen zonder een duidelijke of legitieme reden, of indien de betalingsstructuur ongebruikelijk lijkt, moet u de transactie weigeren, overwegen om de zakelijke relatie te beëindigen en een melding doen aan de CFI.

Documenteer altijd de reden waarom u contante betalingen aanvaardt of weigert, en zorg ervoor dat alle wettelijke limieten strikt worden nageleefd. Deze informatie moet op verzoek beschikbaar zijn, bijvoorbeeld tijdens een AML-controle.

Wat moet u doen wanneer een tegenpartij aandringt op een contante betaling?

- Beoordeel of het gevraagde cashbedrag binnen de wettelijke limiet valt (België: €3.000).
- Indien het bedrag de limiet overschrijdt: weiger onmiddellijk.
- Indien het bedrag binnen de limiet valt maar ongebruikelijk of ongerechtvaardigd lijkt voor de transactie: pas EDD toe — vraag om een uitleg en verifieer de oorsprong van de fondsen.
- Documenteer uw beslissing — ongeacht of u de betaling aanvaardt of weigert — en de redenen daarvoor.
- Indien u geen bevredigende uitleg kan verkrijgen, weiger dan de betaling en beoordeel of een melding aan de CFI vereist is.

Praktisch voorbeeld

Tijdens een lopende zakelijke relatie laat een klant met wie u al twee jaar samenwerkt weten dat hij €10.000 in contanten wil betalen voor zijn laatste aankoop. Tot nu toe ontving u altijd bankoverschrijvingen van deze klant.

Stap 1 — Wettelijke controle: €10.000 in contanten in België overschrijdt de wettelijke limiet van €3.000. Dit is geen beoordelingskwestie — het is wettelijk verboden.

Stap 2 — Weigeren: U moet de contante betaling weigeren, ongeacht uw bestaande relatie of eerdere risicoclassificatie van de klant.

Stap 3 — Herbeoordeling van de relatie: Het verzoek op zich is een alarmsignaal en moet aanleiding geven tot een herbeoordeling van het risicoprofiel van de klant. Een klant die eerder als “laag risico” werd beschouwd, blijft geen laag risico wanneer hij om iets illegaals vraagt.

Stap 4 — Documenteren: Registreer het verzoek, uw weigering en de redenen daarvoor.

Stap 5 — Melden indien nodig: Indien het verzoek wijst op verdachte intenties, meld dit aan de CFI.

Doe de risicoanalyse-check:

Zorg ervoor dat u duidelijk antwoord kan geven op de volgende vragen:

- Wie is de tegenpartij? (KYC)
- Wie bezit de tegenpartij? (UBO's geïdentificeerd en geverifieerd)
- Waarom doet u zaken? (doel en aard van de zakelijke relatie)
- Zijn er alarmsignalen? (PEP, sancties, hoogrisicoland, betaling via derden, contante betaling)
- Kunnen de risico's worden beperkt? – Via EDD-maatregelen en/of interne goedkeuring door het senior management
- Zijn de transacties logisch? – Stemmen ze overeen met het profiel en de bedrijfsactiviteiten van de tegenpartij?
- Wat is uw beslissing? Aanvaarden, aanvaarden onder voorwaarden of weigeren.

Documenteer dit schriftelijk!

Test uw kennis

(de correcte antwoorden vindt u achteraan in deze syllabus)

1. Tijdens een zakelijke relatie wil een klant u €10.000 in contanten betalen in België. Wat doet u?
 - a. Weigeren, de relatie indien gepast beëindigen en melden aan de CFI — contante betalingen van deze omvang zijn verboden in België
 - b. Aanvaarden — er bestaat geen cashlimiet in België, maar behandel de klant als hoog risico
 - c. Aanvaarden indien het bedrag lager is dan €20.000 en uw risicoanalyse actualiseren
 - d. De klant werd eerder beoordeeld als laag risico, dus er verandert niets
2. Welke persoon kan beschouwd worden als een PEP (Politically Exposed Person)?
 - a. Personen die strafrechtelijk werden aangeklaagd — middel tot hoog risico; verhoogde waakzaamheid vereist
 - b. Personen die een prominente publieke functie bekleden of hebben bekleed — middel tot hoog risico; verhoogde waakzaamheid vereist
 - c. Personen die een prominente publieke functie bekleden of hebben bekleed — het is verboden om zaken met hen te doen
 - d. Personen die strafrechtelijk werden aangeklaagd — het is verboden om zaken met hen te doen
3. Een diamanthandelaar stelt een ongebruikelijke transactie vast — bijvoorbeeld een uitzonderlijk grote aankoop. Wat moet de handelaar doen?
 - a. De tegenpartij als laag risico behandelen
 - b. Het negeren tenzij er rechtstreeks bewijs van witwassen bestaat
 - c. Intern bespreken maar geen verdere actie ondernemen en niets schriftelijk registreren
 - d. De klant om uitleg vragen maar geen verder onderzoek uitvoeren — privacywetgeving verhindert dit
 - e. Onderzoek uitvoeren en een schriftelijke analyse opstellen. Indien witwassen wordt vermoed, melden aan de CFI
4. Een klant stelt voor om via een derde partij te betalen. Hoe reageert u?
 - a. Aanvaarden via een erkende tussenpersoon zonder documentatie te vereisen
 - b. De betaling weigeren en de klant vragen naar de reden en de oorsprong van de fondsen; verifiëren voordat u verdergaat
 - c. Weigeren en de klant informeren dat enkel rechtstreekse bankoverschrijvingen zijn toegestaan; onmiddellijk melden aan de CFI
 - d. Aanvaarden zolang het bedrag onder de cashdrempel van €3.000 blijft

5. Indien een hoogrisicoklant geen verdachte activiteiten vertoont, hoeft zijn dossier enkel te worden geactualiseerd wanneer zich een ongebruikelijke gebeurtenis voordoet.
- a. True
 - b. False
6. Er staan momenteel 3 landen op de FATF-zwarte lijst: Noord-Korea en Iran. Welk is het derde?
7. Welk type diamant valt NIET onder de EU-sancties op Russische diamanten?
- a. Geslepen diamanten van meer dan 0,5 karaat
 - b. Synthetische (lab-grown) diamanten van meer dan 0,5 karaat
 - c. Industriële diamanten van meer dan 0,5 karaat
 - d. Ruwe diamanten van meer dan 0,5 karaat
8. Diamanten die vermoedelijk van Russische oorsprong zijn missen de correcte documentatie. Wat gebeurt er?
- a. In quarantaine geplaatst en getest
 - b. Teruggestuurd naar het exporterende land
 - c. Behandeld als verboden goederen — de douane start een onderzoek
 - d. Tijdelijk toegelaten in afwachting van verduidelijking
9. Een Belgische handelaar koopt in 2024 Russische ruwe niet-industriële diamanten (>0,5 ct) van een handelaar in Dubai. Dit is toegestaan omdat de goederen uit de VAE komen.
- a. True
 - b. False
10. Op welke datum trad het EU-verbod op Russische niet-industriële diamantimporten in werking?
11. Welke Belgische overheidsdienst is verantwoordelijk voor het toezicht op de financiële sancties opgelegd door de EU?
- a. FPS Finance
 - b. CFI
 - c. FPS Economy

Hoofdstuk 5: Melden van verdachte activiteiten

Wat leer ik in dit hoofdstuk?

5.1 Wat is het melden van verdachte activiteiten en waarom is het belangrijk?

5.2 Wanneer moet u verdachte activiteiten melden?

5.3 Bescherming van de meldende persoon door de overheid

5.4 Waar en hoe moet u verdachte activiteiten melden?

5.1

Wat is het melden van verdachte activiteiten en waarom is het belangrijk?

Indien een transactie of zakelijke relatie ongebruikelijk, inconsistent of verdacht lijkt — zelfs indien u geen bewijs van onrechtmatig handelen hebt — moet u de transactie stopzetten en dit zonder uitstel melden aan de CFI (Cel voor Financiële Informatieverwerking).

Dit wordt het melden van verdachte activiteiten genoemd en het is een wettelijke verplichting.

Opgelet

De beslissing om een transactie niet voort te zetten en de CFI te informeren moet duidelijk schriftelijk worden gedocumenteerd. U moet tijdens een AML-controle ook een overzicht kunnen voorleggen van alle meldingen die aan de CFI werden gedaan. Merk op dat het, waar van toepassing, in uw voordeel werkt om aan te tonen dat u dergelijke meldingen hebt gemaakt.

Het melden van verdachte activiteiten is belangrijk omdat het helpt om:

- Witwassen en terrorismefinanciering op te sporen en te voorkomen
- Uw onderneming te beschermen tegen juridische en reputatierisico's
- Bij te dragen aan de integriteit en transparantie van de diamantsector

5.2

Wanneer moet u verdachte activiteiten melden?

U beslist of u een melding moet doen aan de Cel voor Financiële Informatieverwerking (CFI) op basis van de risicoanalyse die u hebt uitgevoerd voor deze specifieke klant, leverancier of transactie, met behulp van de risicoscorekaarten (zie bijlage A, B en C).

U moet een melding doen aan de CFI indien:

- Uw risicoanalyse minstens één onaanvaardbaar (rood) risico identificeert (zie bijlage A, B of C), of
- Meerdere risicofactoren het onveilig maken om verder te gaan

In dergelijke gevallen moet de tegenpartij worden geweigerd of moet de bestaande relatie worden beëindigd en moet de Cel voor Financiële Informatieverwerking (CFI) worden geïnformeerd:

- vóór de transactie wordt uitgevoerd, waarbij u de verwachte timing van de transactie moet vermelden.
- onmiddellijk nadien (indien vooraf melden niet mogelijk was), waarbij u duidelijk moet uitleggen waarom voorafgaande melding niet mogelijk was.

Opgelet

Het is verboden om uw tegenpartij of andere derden te informeren over het feit dat u een melding hebt gedaan aan de CFI.

U moet een melding doen telkens wanneer een situatie ongebruikelijk, inconsistent of verdacht lijkt, zelfs indien u geen bewijs hebt van onrechtmatig handelen.

Voorbeelden:

- De oorsprong van de fondsen is onduidelijk of kan niet worden geverifieerd: Bijvoorbeeld wanneer de tegenpartij niet kan uitleggen waar het geld vandaan komt of tegenstrijdige informatie verstrekt.
- De transactie heeft geen economisch of logisch doel: Bijvoorbeeld het kopen of verkopen van diamanten zonder duidelijke zakelijke reden.
- De tegenpartij weigert informatie of documenten te verstrekken: Een gebrek aan transparantie is een sterke risico-indicator.
- Er zijn aanwijzingen van structurering of pogingen om wettelijke limieten te omzeilen: Bijvoorbeeld het opsplitsen van contante betalingen om onder de wettelijke drempel te blijven.
- Er worden ongebruikelijke betaalmethoden gebruikt: Zoals betalingen door derden zonder duidelijke rechtvaardiging.
- De tegenpartij is gelinkt aan criminele activiteiten, sancties of negatieve berichtgeving in de media: Dit omvat fraude, corruptie, belastingontduiking of andere illegale activiteiten.
- U vermoedt het gebruik van valse of vervalste documenten.
- De transactie omvat hoogrisicolanden zonder duidelijke verklaring.
- De tegenpartij dringt aan op geheimhouding of ongebruikelijke vertrouwelijkheid.

Opgelet

U moet ook pogingen tot transacties melden, zelfs indien deze niet werden voltooid.

5.3

Bescherming van de meldende persoon door de overheid

De diamanthandelaar (of elke werknemer) die te goeder trouw een melding indient, wordt door de autoriteiten beschermd tegen bedreigingen of daden van agressie.

De Cel voor Financiële Informatieverwerking behandelt alle meldingen vertrouwelijk en deelt deze niet met derden.

Iedereen die te goeder trouw informatie verstrekt of een melding doet, kan hiervoor op geen enkele manier worden gestraft of aansprakelijk worden gesteld (burgerrechtelijk, strafrechtelijk of disciplinair) en geniet dus wettelijke bescherming (dit wordt 'wettelijke immuniteit' genoemd).

5.4

Waar en hoe verdachte activiteiten melden?

In België moeten verdachte activiteiten worden gemeld aan de Cel voor Financiële Informatieverwerking (CFI) / Cellule de Traitement des Informations Financières (CTIF).

Meldingen aan de Cel voor Financiële Informatieverwerking (CFI) moeten worden ingediend via de goAML-applicatie.

Hiervoor moet u zich eerst registreren en een account aanmaken door een aanvraag te sturen naar goaml.helpdesk@ctif-cfi.be.

Het is de verantwoordelijkheid van de AML-verantwoordelijke om een account aan te maken op goAML en verdachte transacties te melden aan de CFI.

Uw meldingsrapport moet het volgende bevatten:

- Wie de tegenpartij is (identificatiegegevens)
- Wat de transactie inhoud
- Waarom deze verdacht leek
- Eventuele ondersteunende documenten

Belangrijke principes die moeten worden nageleefd

- Wacht niet tot u 100% zeker bent: een vermoeden volstaat om een melding te doen, u heeft geen bewijs van onrechtmatig handelen nodig.
- Informeer de tegenpartij niet (geen 'tipping-off'): het is strikt verboden om de tegenpartij te informeren dat er een melding werd gedaan.
- Handel zonder uitstel: meldingen moeten gebeuren zodra het vermoeden ontstaat en vóór de transactie plaatsvindt.
- U bent beschermd en kan op geen enkele manier worden gestraft of aansprakelijk worden gesteld (melden te goeder trouw geeft u wettelijke immuniteit).

Praktisch voorbeeld 1

Een klant wil een geslepen diamant kopen voor €8.500. Hij stelt het volgende voor:
€2.900 in contanten vandaag
€2.900 in contanten morgen
Het resterende bedrag later, opnieuw in contanten

Zelfs nadat u hem informeert dat de wettelijk toegestane limiet voor contante betalingen in België €3.000 bedraagt, blijft hij aandringen op het opsplitsen van de betalingen en vermeldt hij expliciet dat hij “onder de limiet wil blijven”.

→ Dit is een duidelijk voorbeeld van structurering: het bewust opsplitsen van een transactie in kleinere bedragen om wettelijke limieten of controles te omzeilen (in dit geval de Belgische limiet van €3.000 voor contante betalingen).

Waarom melden aan de CFI?

Duidelijke poging om de wettelijke limiet voor contante betalingen te omzeilen

De betalingsstructuur is artificieel en heeft geen economische rechtvaardiging

Wijst op een mogelijke poging om de oorsprong van fondsen te verbergen of traceerbaarheid te vermijden

Ook al ligt elke afzonderlijke betaling onder €3.000, de intentie om de wet te omzeilen is expliciet, wat een sterk vermoeden creëert.

Praktisch voorbeeld 2

Een nieuwe leverancier gevestigd in Zuid-Afrika (dat sinds 2023 op de FATF-grijze lijst staat wegens tekortkomingen in de bestrijding van witwassen en het waarborgen van transparantie) biedt een partij ruwe diamanten aan tegen een aantrekkelijke prijs.

Tijdens de onboarding:

De leverancier verstrekt onvolledige KYC-informatie

Er is geen duidelijke documentatie over de oorsprong van de diamanten

Wanneer bijkomende informatie wordt gevraagd, reageert de leverancier ontwijkend en dringt hij aan om snel verder te gaan

→ Waarom is dit een hoog risico? Landen op de FATF-grijze lijst worden geïdentificeerd als landen met strategische tekortkomingen in hun AML/CFT-kader, wat het risico op witwassen of illegale handel verhoogt.

Waarom melden aan de CFI?

Tegenpartij gevestigd in een jurisdictie met een hoger risico (FATF-grijze lijst)

Gebrek aan transparantie zowel over de leverancier (onvolledig KYC-dossier) als over de goederen (geen documentair bewijs van oorsprong)

Druk om verder te gaan ondanks ontbrekende of onduidelijke informatie

→ De combinatie van geografisch risico + onvolledige KYC + ontwijkend gedrag creëert een redelijk vermoeden van witwassen of illegale oorsprong van goederen, wat een meldingsplicht doet ontstaan.

Test uw kennis

(juiste antwoorden worden aan het einde van deze syllabus gegeven)

1. Ben ik wettelijk verplicht om verdachte transacties te melden aan de CFI?
 - a. Ja. Ik ben verplicht dit te doen en geniet immuniteit — er bestaat geen risico op vervolging
 - b. Nee. Melden is vrijwillig
 - c. Ja, maar enkel voor transacties boven een bepaald bedrag of afkomstig uit bepaalde landen
 - d. Ja, maar enkel indien ik zeker ben dat er sprake is van witwassen

Hoofdstuk 6: Hoe bereidt u zich voor op een AML-controle

Wat leer ik in dit hoofdstuk?

6.1 Wat is een AML-controle?

6.2 Hoe verloopt een AML-controle?

6.3 Welke informatie moet u kunnen voorleggen?

6.4 Praktische tips en tricks om een AML-controle succesvol door te komen

6.1 Wat is een AML-controle?

Een AML-controle is een officieel bezoek van een inspecteur van de FPS Economy.

Tijdens de controle gaat de inspecteur na of uw onderneming de AML-wetgeving naleeft in haar dagelijkse werking, inclusief de correcte toepassing van KYC, risicoanalyses, interne procedures en de melding van verdachte activiteiten.

Een controle is niets om bang voor te zijn als u goed voorbereid bent. Indien uw dossiers volledig zijn, uw processen duidelijk zijn en u de AML-wetgeving begrijpt, bevestigt een controle eenvoudigweg dat uw onderneming werkt zoals het hoort.

Een AML-controle is geen eenmalige momentopname, maar een rechtstreekse weerspiegeling van hoe uw onderneming elke dag functioneert.

6.2 Hoe verloopt een AML-controle?

Tijdens een controle zal de inspecteur doorgaans:

- Ongeveer 20 tot 30 klant- of leveranciersdossiers selecteren (tot 3 jaar terug)
- Controleren of uw AML-dossiers volledig en goed georganiseerd zijn
- Controleren of u correcte risicoanalyses hebt uitgevoerd
- Controleren of u hoogrisicotegenpartijen correct identificeert
- U vragen om uw beslissingen toe te lichten (bijvoorbeeld waarom u een tegenpartij hebt aanvaard)
- Controleren of uw KYC-informatie up-to-date is
- Controleren of u de limieten voor contante betalingen en de meldingsplicht van verdachte transacties naleeft

De controle kan meerdere uren duren — soms een volledige werkdag. Hoe beter uw dossiers georganiseerd zijn, hoe sneller de controle verloopt.

Opgelet

De AML-verantwoordelijke(n) is/zijn verantwoordelijk voor het begeleiden van de controle, het beantwoorden van vragen en het voorleggen van de gevraagde documenten. Indien de AML-verantwoordelijke(n) niet aanwezig is/zijn, moet een andere werknemer deze rol kunnen overnemen en de inspecteurs van informatie kunnen voorzien.

Tijdens de controle zal de inspecteur u vragen verschillende documenten voor te leggen. Zorg ervoor dat u deze allemaal gemakkelijk en fysiek toegankelijk hebt, zodat de controle efficiënt kan verlopen.

Dit is een checklist van alle documenten die op verzoek van de inspecteur onmiddellijk beschikbaar moeten zijn:

- De namen van de uiteindelijke AML-verantwoordelijke (op senior managementniveau) en de 'operationele' AML-verantwoordelijke die verantwoordelijk is voor de praktische uitvoering van de AML-procedures op dagelijkse basis.
- Een intern AML-beleid, jaarlijks bijgewerkt en ondertekend (u kan gebruikmaken van het AML Policy Template ontwikkeld door Antwerp World Diamond Centre; zie hoofdstuk 7 – AML-templates, tools en handleidingen aangeboden door AWDC).
- Uw AML-certificaat, als bewijs dat u jaarlijks het AML-webinar hebt gevolgd of geslaagd bent voor het AML-examen.
- Een volledig AML-dossier voor elke tegenpartij, inclusief KYC-informatie, een risicoanalyse en een gedocumenteerde conclusie over hoe verder te gaan met de zakelijke relatie (aanvaarden, aanvaarden onder voorwaarden of weigeren). (U kan gebruikmaken van de KYC and Risk Assessment Conclusion Template ontwikkeld door Antwerp World Diamond Centre; zie hoofdstuk 7 – AML-templates, tools en handleidingen aangeboden door AWDC).
- Historische AML-dossiers voor elke tegenpartij.
- Een fysieke of digitale kopie van uw AML Activity Report.
- Facturen die een periode van maximaal drie jaar bestrijken.
- Kasboeken. Indien deze niet fysiek beschikbaar zijn op uw kantoor, kan de inspecteur deze rechtstreeks opvragen bij uw accountant of boekhouder.

Opgelet

Naast het controleren van uw documentatie zullen inspecteurs ook uw kennis van de AML-wetgeving testen door praktische vragen te stellen. Deze kunnen onder meer betrekking hebben op wat als een verdachte transactie wordt beschouwd, hoe u met een dergelijke situatie zou omgaan, wat een UBO (Ultimate Beneficial Owner) is en wat de rol van de CFI is. Het is daarom essentieel om niet alleen uw documenten op orde te hebben, maar ook om de AML-verplichtingen en de praktische toepassing ervan duidelijk te begrijpen.

6.4

Praktische tips en tricks om een AML-controle succesvol door te komen

Zorg ervoor dat u te allen tijde goed voorbereid bent op een AML-controle. Inspecteurs kunnen op elk moment langskomen, vaak zonder voorafgaande aankondiging.

De volgende tips helpen u om een controle vlot te laten verlopen en de duur ervan zo kort mogelijk te houden:

- Zorg ervoor dat u beschikbaar bent voor inspecteurs van de FPS Economy en aanwezig bent op het geregistreerde adres van uw onderneming. Indien u herhaaldelijk afwezig bent of een controle weigert, kan een proces-verbaal worden opgesteld.
- Houd alle vereiste informatie goed georganiseerd en gemakkelijk toegankelijk. Zo vermijdt u dat u tijdens de controle documenten moet zoeken, wat onnodige stress kan veroorzaken en het proces kan vertragen. Werken met een digitale tool zoals KYCP kan helpen om uw documenten te structureren, op te slaan en up-to-date te houden (zie hoofdstuk 7 – AML-templates, tools en handleidingen aangeboden door AWDC).
- Wees altijd eerlijk en transparant. Probeer fouten niet te verbergen of te minimaliseren en aarzel niet om toe te geven wanneer iets niet perfect is.
- Zorg ervoor dat u de AML-wetgeving begrijpt. Inspecteurs kunnen theoretische vragen stellen waarop u moet kunnen antwoorden, zoals wat een UBO is of wat de rol is van de Cel voor Financiële Informatieverwerking.
- Toon aan dat u meldingen hebt gedaan aan de CFI wanneer dat nodig was. Het werkt in uw voordeel indien u kan aantonen dat u dergelijke meldingen hebt gemaakt wanneer vereist.
- Toon voortdurende monitoring aan. Demonstreer dat u uw zakelijke relaties regelmatig herbekijkt en AML-informatie up-to-date houdt.
- Leid uw personeel op. Zorg ervoor dat werknemers uw interne AML-procedures kennen en regelmatig worden bijgewerkt.

Opgelet

Tijdens een controle is het de verantwoordelijkheid van één van de AML-verantwoordelijken om de vragen van de inspecteur te beantwoorden en de gevraagde documenten voor te leggen. Indien geen van beiden aanwezig is, moet een andere werknemer deze rol kunnen overnemen.

Test uw kennis

(juiste antwoorden worden aan het einde van deze syllabus gegeven)

1. Een AML-controle wordt vooraf aangekondigd zodat u tijd heeft om uw dossiers voor te bereiden.
 - a. Juist
 - b. Onjuist

2. Tijdens een AML-controle selecteert de inspecteur een aantal tegenpartijdossiers om te controleren. Hoeveel dossiers worden doorgaans geselecteerd en hoe ver kunnen deze teruggaan?
 - a. 5 tot 10 dossiers, tot 1 jaar terug
 - b. 20 tot 30 dossiers, tot 3 jaar terug
 - c. 50 tot 100 dossiers, tot 5 jaar terug
 - d. Alle dossiers van het afgelopen jaar

3. De AML-verantwoordelijke is niet beschikbaar op de dag van een controle. Wat gebeurt er?
 - a. De controle wordt automatisch uitgesteld totdat de AML-verantwoordelijke aanwezig is
 - b. De controle kan niet doorgaan — enkel de AML-verantwoordelijke is wettelijk bevoegd om te antwoorden
 - c. Een andere werknemer moet de rol kunnen overnemen en de inspecteur de gevraagde informatie kunnen bezorgen
 - d. De onderneming kan de documenten binnen de 5 werkdagen per e-mail bezorgen

4. Welke van de volgende zaken kan een inspecteur NIET vragen tijdens een AML-controle?
 - a. U vragen uit te leggen waarom u een specifieke tegenpartij hebt aanvaard
 - b. Uw AML-certificaat voorleggen
 - c. Aantonen dat u verdachte transacties aan de CFI hebt gemeld wanneer vereist
 - d. Een lijst bezorgen van alle transacties boven €1.000 van de afgelopen 10 jaar

Hoofdstuk 7: AML-templates, tools en handleidingen aangeboden door AWDC

Wat leer ik in dit hoofdstuk?

7.1 Ready-to-use AML templates

7.2 Tools

7.3 Handleidingen

AWDC biedt drie gebruiksklare templates aan. Alle templates zijn goedgekeurd door of ontwikkeld in overeenstemming met de vereisten van de FPS Economy.

AML Policy Template:

Deze Anti-Money Laundering (AML) Policy Template werd opgesteld als een praktische leidraad om in België geregistreerde diamantbedrijven te helpen bij het opstellen van hun intern AML-beleid. De template werd goedgekeurd door de FPS Economy en moet worden aangepast aan de specifieke situatie van elke onderneming.



AML Client Letters:

AML Client Letters zijn standaardbrieven die u naar uw klanten of leveranciers kan sturen wanneer u KYC-informatie van hen nodig heeft. Vraag hen om de ontbrekende informatie aan te vullen en het document terug naar u te sturen.



KYC and Risk Assessment Conclusion Template:

U kan deze template gebruiken om uw beslissing om een tegenpartij te aanvaarden, onder voorwaarden te aanvaarden of te weigeren duidelijk te motiveren en te documenteren.



7.2.1 KYCP: een essentiële AML-tool voor diamanthandelaren

Om diamanthandelaren te helpen voldoen aan de AML-wetgeving, biedt Antwerp World Diamond Centre verschillende praktische tools aan. De belangrijkste daarvan is KYCP (Know Your Customer Platform).

KYCP is een online platform dat u helpt om alle AML-gerelateerde informatie over uw tegenpartijen centraal te verzamelen, beheren en actualiseren. Het ondersteunt u gedurende het volledige due diligence-proces:

- Uw tegenpartijen identificeren en verifiëren
- Hun risicoprofiel beoordelen
- AML-documenten en informatie up-to-date houden
- Uw beslissingen documenteren en motiveren (aanvaarden, weigeren of een relatie beëindigen)

Geïntegreerde screeningtools: GRID en ORBIS

Wanneer u KYCP gebruikt, krijgt u ook toegang tot krachtige databanken en screeningtools die volledig geïntegreerd zijn in de KYCP-module:

- ORBIS: een wereldwijde bedrijfsdatabank die gedetailleerde informatie verstrekt over ondernemingen, waaronder:
 - Eigendomstructuren (inclusief UBO's)
 - Financiële gegevens
 - Bedrijfsstructuren en corporate links

Dit helpt u om beter te begrijpen met wie u zaken doet.

GRID: een uitgebreide databank die wordt gebruikt om tegenpartijen te screenen en monitoren op risico's met betrekking tot financiële criminaliteit. Deze bevat gegevens over:

- Politically Exposed Persons (PEP's)
- Sanctielijsten
- Negatieve berichtgeving in de media

Samen ondersteunen deze tools een volledig, consistent en goed gedocumenteerd risicoanalyseproces. Ze helpen u te beslissen of u een tegenpartij al dan niet kan onboarden.

Indien u reeds een KYCP-account heeft, kan u hier inloggen:



Indien u nog niet geregistreerd bent voor KYCP, vraag dan uw gratis account aan via compliance@awdc.be. Voor meer informatie over KYCP, bezoek onze website via de QR-code hieronder.

Nieuw bij KYCP? Bekijk onze korte video via de QR-code hieronder — deze begeleidt u stap voor stap door het registratieproces en toont wat KYCP voor u kan betekenen.



7.2.2 UBO-register (Ultimate Beneficial Owners)

Het Belgische UBO-register bevat de uiteindelijke begunstigten (Ultimate Beneficial Owners), volledig of gedeeltelijk, van alle Belgische ondernemingen, vzw's, stichtingen en trusts.

Gebruik dit register om te verifiëren wie een Belgische onderneming waarmee u zaken wenst te doen werkelijk bezit of controleert.



7.2.3 Tools om u te helpen bij handel met gesanctioneerde landen

Indien u wilt beoordelen of het veilig is om zaken te doen met een tegenpartij gevestigd in een land dat onder sancties of embargo's valt, of in een land dat geen lid is van het Kimberley Process, wordt sterk aanbevolen om deze tools te gebruiken om de risico's verbonden aan de zakelijke relatie te evalueren en te bepalen of het nog mogelijk is om verder te gaan, mits passende risicobeperkende maatregelen worden genomen.

FATF Black and Grey List:

Toont welke landen tekortkomingen hebben in de bestrijding van witwassen en terrorismefinanciering. Landen op de Black List zijn de landen met het hoogste risico (Myanmar, Iran en Noord-Korea), terwijl landen op de Grey List onder verhoogde monitoring staan.



Kimberley Process Participants List:

Toont welke landen deel uitmaken van het Kimberley Process — het internationale certificeringssysteem dat conflictdiamanten uit de markt moet houden. Indien een land niet op deze lijst staat, is extra voorzichtigheid vereist.



7.2.4 CFI-platform om verdachte transacties of feiten te melden

Als diamanthandelaar moet u de CFI altijd informeren wanneer u een verdachte transactie of feit vaststelt dat mogelijk verband houdt met witwassen of financiering van terrorisme.

Meldingen aan de Cel voor Financiële Informatieverwerking (CFI) moeten worden ingediend via de goAML-applicatie.

Hiervoor moet u zich eerst registreren en een account aanmaken door een aanvraag te sturen naar goaml.helpdesk@ctif-cfi.be.

Het is de verantwoordelijkheid van de AML-verantwoordelijke om een account aan te maken op goAML en verdachte transacties te melden aan de CFI.

Dien uw AML-rapport in
Handleiding:



Handleiding: Toegang tot Diamond Supervision (vereist voor het indienen van uw AML-rapport):



KYCP:

Nieuw bij KYCP? Bekijk onze korte video. Deze begeleidt u door het registratieproces en toont wat KYCP voor u kan betekenen.

U vindt de video onderaan deze pagina:



Woordenlijst

A

AML-certificaat

Bewijs van succesvolle voltooiing van een AML-opleiding.

AML-controle

Controle door de FPS Economy waarbij wordt nagegaan of AML-verplichtingen worden nageleefd.

AML-verplichtingen (8 stappen)

De kernverplichtingen inzake compliance voor diamanthandelaren, waaronder opleiding, KYC en risicoanalyse.

AML-verantwoordelijke

De persoon die verantwoordelijk is voor AML-compliance binnen de onderneming (meestal een bestuurder) en erop toeziet dat procedures worden nageleefd en risico's worden gemonitord.

AML-beleid

Intern document waarin wordt uiteengezet hoe uw onderneming voldoet aan de AML-regels.

AML-rapport (jaarlijks)

Een jaarlijks rapport dat via het overheidsplatform wordt ingediend en een overzicht geeft van de AML-activiteiten.

AML-meldingsprocedure

Intern proces waarin wordt uitgelegd hoe en wanneer verdachte activiteiten moeten worden gemeld.

AML-seminarie

Verplichte jaarlijkse opleiding over AML-compliance.

Anti-Money Laundering (AML)-wetgeving

Wettelijk kader dat ondernemingen verplicht om witwassen te voorkomen, op te sporen en te melden door middel van KYC, risicoanalyse en meldingsverplichtingen.

B

Faillissement (Eng: bankruptcy)

Een juridische procedure waarbij een persoon of onderneming die haar schulden niet meer kan betalen insolvent wordt verklaard en haar activa worden gebruikt om schuldeisers terug te betalen.

Best Practice Seminarie

Optionele opleiding gericht op transparantie en goede praktijken.

C

Cel voor Financiële Informatieverwerking (CFI)

Belgische financiële inlichtingeneenheid die meldingen van verdachte activiteiten ontvangt en analyseert.

Klant (Eng: Client)

Een persoon of onderneming aan wie u verkoopt.

Complexe eigendomsstructuur

Een bedrijfsstructuur met meerdere lagen van eigenaars of entiteiten, waardoor het moeilijk is om te achterhalen wie de onderneming werkelijk controleert.

E

Enhanced due diligence (EDD)

Bijkomende controles die vereist zijn voor hoogrisicoklanten (bv. PEP's of klanten uit hoogrisicolanden).

G

General Data Protection Regulation (GDPR)

(General Data Protection Regulation): Een EU-wetgeving die de persoonsgegevens en privacy van personen beschermt.

H

Hoogrisicoklant

Een klant die bijkomende controle vereist (bv. PEP's, hoogrisicolanden of ongebruikelijke transacties).

Hoogrisicoland

Een land dat wordt geïdentificeerd als een land met een verhoogd risico op witwassen of zwakke AML-controles.

I

Itsme

Een beveiligde app die in België wordt gebruikt om uw identiteit te verifiëren en in te loggen op officiële diensten.

K

KYC (Know Your Customer / Counterparty)

Het proces waarbij klanten en leveranciers worden geïdentificeerd en geverifieerd, hun activiteiten worden begrepen en hun risico wordt beoordeeld.

KYC file

Een gedocumenteerd dossier dat aantoont dat u:

- Uw tegenpartij kent
- De relatie begrijpt
- Het risico hebt beoordeeld
- Uw beslissing hebt gemotiveerd

KYCP (Know Your Counterparty Platform)

Digitale tool voor het beheren van KYC, het screenen van risico's en het monitoren van klanten.

M

Moody's

Een financieel platform dat kredietratings en risicoanalyses verstrekt voor ondernemingen en overheden.

Money laundering

Het proces waarbij de illegale oorsprong van geld wordt verborgen om het legitiem te laten lijken.

MyMinFin

Een online platform van de Belgische overheid waarop u uw belastingen en financiële informatie beheert.

N

Natuurlijke persoon

De onderneming wordt uitgebaat door een individu zonder afzonderlijke rechtspersoon, zoals een vennootschap.

Niet-naleving

Het niet voldoen aan AML-verplichtingen → kan leiden tot boetes of sancties.

O

Voortdurende monitoring (Eng: Ongoing monitoring)

Doorlopende controle van klanten/leveranciers tijdens de zakelijke relatie om ervoor te zorgen dat het risico aanvaardbaar blijft.

P

Politically Exposed Person (PEP)

Een persoon met een prominente publieke functie (bv. minister), inclusief diens familieleden en nauwe associates, die als een hoger risico wordt beschouwd.

R

Bewaarplicht (Eng: Record Keeping)

Verplichting om AML-/KYC-gegevens gedurende 10 jaar te bewaren na het einde van de zakelijke relatie.

Red flags

Waarschuwingssignalen voor mogelijk witwassen, zoals:

- Ongebruikelijke betaalmethoden
- Gebrek aan transparantie
- Intensief gebruik van contant geld
- Complexe eigendomsstructuren

Registered Diamond Companies (.be)

Overheidsplatform voor AML-rapportering, opleidingen en bedrijfsregistratie.

Risicoanalyse

Het proces waarbij wordt beoordeeld of een klant of leverancier een risico vormt voordat een zakelijke relatie wordt aangegaan.

Role Management Administration (RMA)

Een systeem dat wordt gebruikt om gebruikersrollen en toegangsrechten toe te wijzen, te beheren en te controleren binnen overheidsplatformen (bv. MyMinFin), zodat enkel bevoegde personen toegang hebben tot en specifieke administratieve of compliance-gerelateerde taken kunnen uitvoeren namens een onderneming.

S

Sancties

Beperkingen opgelegd door overheden of internationale instanties die zakelijke relaties met bepaalde personen, entiteiten of landen verbieden.

Sanctiehit

Een overeenkomst tussen uw tegenpartij en een sanctielijst → de zakelijke relatie moet onmiddellijk worden stopgezet.

Verschil met een PEP:

- PEP = toegestaan mits verhoogde voorzichtigheid
- Gesanctioneerde persoon = verboden

Sanctielijsten

Officiële lijsten (EU, VN, OFAC) van gesanctioneerde personen en entiteiten.

Sanctiescreening

Het proces waarbij wordt gecontroleerd of een klant, leverancier of UBO voorkomt op een sanctielijst.

Leverancier (Eng: Supplier)

Een persoon of onderneming van wie u aankoopt.

Supply Chain Due Diligence (SCDD)

Proces waarbij wordt nagegaan of diamanten op ethische wijze zijn verkregen (mensenrechten, conflictvrij, enz.).

SCDD vs AML

- AML → financiële criminaliteit
- SCDD → ethische herkomst

Melding van verdachte transacties (STR) (Eng: Suspicious Transaction Report)

Een verplichte melding die wordt ingediend wanneer u witwassen of criminele activiteiten vermoedt.

T

Third-party payment

Een betaling uitgevoerd door iemand anders dan de gefactureerde klant; wordt beschouwd als een hoog risico en vereist een rechtvaardiging.

U

Ultimate Beneficial Owner (UBO)

De natuurlijke perso(o)n(en) die een onderneming uiteindelijk bezit(ten) of controleert/controleren ($\geq 25\%$ eigendom of controle).

Verbetersleutel

Hoofdstuk 1

1. Wat is het maximumbedrag van de boete voor een rechtspersoon onder de Belgische antiwitwaswetgeving in geval van niet-naleving door een diamanthandelaar?
 - a. 1.000.000 euro
 - b. 2.000.000 euro
 - c. 3.000.000 euro
 - d. 1.250.000 euro

2. Welke Belgische overheidsdienst is verantwoordelijk voor het uitvoeren van AML-controles?
 - a. FOD Financiën
 - b. CFI
 - c. FOD Economie

Hoofdstuk 2

1. Wat is de deadline voor het indienen van het jaarlijkse AML-verslag?
 - a. 1 april
 - b. 31 maart
 - c. 31 mei
 - d. 1 juni

2. Hoe vaak moet u een AML-opleiding volgen als u niet geslaagd bent voor het AML-examen?
 - a. Elk jaar
 - b. Om de twee jaar
 - c. Om de drie jaar
 - d. Om de vier jaar

3. Een AML-verantwoordelijke kan zelfstandig beslissen om bedrijfsmiddelen te gebruiken om aan AML-verplichtingen te voldoen.
 - a. Juist
 - b. Onjuist

4. Alleen de AML-verantwoordelijke (of de door het management aangestelde persoon) kan het jaarlijkse AML-verslag opstellen.
 - a. Juist
 - b. Onjuist

5. Welke Belgische overheidsinstantie houdt toezicht op EU-financiële sancties?
FOD Financiën

6. Hoeveel keer per jaar moet u een AML-opleiding volgen als u niet geslaagd bent voor het examen? (Geef een getal) 1

Hoofdstuk 3

1. Een klant weigert een identiteitsdocument te verstrekken of de namen van de UBO's bekend te maken. Wat doet u?
 - a. De relatie voortzetten, de weigering documenteren en uw risicoanalyse aanpassen
 - b. De privacy van de klant respecteren en de relatie voortzetten
 - c. De relatie of transactie weigeren. Indien witwassen wordt vermoed, melden aan de CFI
 - d. De relatie voortzetten maar melden aan de federale gerechtelijke politie
2. Hoe lang moeten documenten worden bewaard nadat een zakelijke relatie is beëindigd? 10 jaar. Hierna dienen de document verwijderd of vernietigd te worden.
3. Uw opzoeking levert geen informatie op over een tegenpartij. Wat doet u?
 - a. De tegenpartij als laag risico beschouwen
 - b. De tegenpartij als neutraal risico beschouwen en de zoekpoging documenteren
 - c. Niet verdergaan — u kunt niet voldoen aan uw identificatieverplichting
 - d. Verdergaan zonder bijkomende verificatie
4. Welke stappen moet een diamanthandelaar volgen om de UBO's van een buitenlandse onderneming te identificeren?
 - a. De onderneming of vertegenwoordiger vragen een verklaring te ondertekenen
 - b. Redelijke stappen ondernemen om informatie te verzamelen en te verifiëren (naam, adres, bestuurders, UBO's) en de documenten bewaren
 - c. Enkel informatie over bestuurders verzamelen indien het risico hoog is
 - d. Enkel naam en adres verzamelen — meer vragen zou in strijd zijn met de GDPR
5. KYC-gegevens moeten elk jaar worden bijgewerkt voor hoogerisicoklanten, en om de 2 tot 3 jaar voor andere klanten.
 - a. Juist
 - b. Onjuist
6. Welk minimumpercentage van eigendom kwalificeert iemand als een UBO in België? 25%

Hoofdstuk 4

1. Tijdens een zakelijke relatie wil een klant u €10.000 in contanten betalen in België. Wat doet u?
 - a. Weigeren, de relatie indien gepast beëindigen en melden aan de CFI — contante betalingen van deze omvang zijn verboden in België
 - b. Aanvaarden — er bestaat geen cashlimiet in België, maar behandel de klant als hoog risico
 - c. Aanvaarden indien het bedrag lager is dan €20.000 en uw risicoanalyse actualiseren
 - d. De klant werd eerder beoordeeld als laag risico, dus er verandert niets
2. Welke persoon kan beschouwd worden als een PEP (Politically Exposed Person)?
 - a. Personen die strafrechtelijk werden aangeklaagd — middel tot hoog risico; verhoogde waakzaamheid vereist
 - b. Personen die een prominente publieke functie bekleden of hebben bekleed — middel tot hoog risico; verhoogde waakzaamheid vereist
 - c. Personen die een prominente publieke functie bekleden of hebben bekleed — het is verboden om zaken met hen te doen
 - d. Personen die strafrechtelijk werden aangeklaagd — het is verboden om zaken met hen te doen
3. Een diamanthandelaar stelt een ongebruikelijke transactie vast — bijvoorbeeld een uitzonderlijk grote aankoop. Wat moet de handelaar doen?
 - a. De tegenpartij als laag risico behandelen
 - b. Het negeren tenzij er rechtstreeks bewijs van witwassen bestaat
 - c. Intern bespreken maar geen verdere actie ondernemen en niets schriftelijk registreren
 - d. De klant om uitleg vragen maar geen verder onderzoek uitvoeren — privacywetgeving verhindert dit
 - e. Onderzoek uitvoeren en een schriftelijke analyse opstellen. Indien witwassen wordt vermoed, melden aan de CFI
4. Een klant stelt voor om via een derde partij te betalen. Hoe reageert u?
 - a. Aanvaarden via een erkende tussenpersoon zonder documentatie te vereisen
 - b. De betaling weigeren en de klant vragen naar de reden en de oorsprong van de fondsen; verifiëren voordat u verdergaat
 - c. Weigeren en de klant informeren dat enkel rechtstreekse bankoverschrijvingen zijn toegestaan; onmiddellijk melden aan de CFI
 - d. Aanvaarden zolang het bedrag onder de cashdrempel van €3.000 blijft

5. Indien een hoogrisicoklant geen verdachte activiteiten vertoont, hoeft zijn dossier enkel te worden geactualiseerd wanneer zich een ongebruikelijke gebeurtenis voordoet.
- a. True
 - b. False
6. Er staan momenteel 3 landen op de FATF-zwarte lijst: Noord-Korea en Iran. Welk is het derde? Myanmar (Burma)
7. Welk type diamant valt NIET onder de EU-sancties op Russische diamanten?
- a. Geslepen diamanten van meer dan 0,5 karaat
 - b. Synthetische (lab-grown) diamanten van meer dan 0,5 karaat
 - c. Industriële diamanten van meer dan 0,5 karaat
 - d. Ruwe diamanten van meer dan 0,5 karaat
8. Diamanten die vermoedelijk van Russische oorsprong zijn missen de correcte documentatie. Wat gebeurt er?
- a. In quarantaine geplaatst en getest
 - b. Teruggestuurd naar het exporterende land
 - c. Behandeld als verboden goederen — de douane start een onderzoek
 - d. Tijdelijk toegelaten in afwachting van verduidelijking
9. Een Belgische handelaar koopt in 2024 Russische ruwe niet-industriële diamanten (>0,5 ct) van een handelaar in Dubai. Dit is toegestaan omdat de goederen uit de VAE komen.
- a. True
 - b. False
10. Op welke datum trad het EU-verbod op Russische niet-industriële diamantimporten in werking? 1 January 2024
11. Welke Belgische overheidsdienst is verantwoordelijk voor het toezicht op de financiële sancties opgelegd door de EU?
- a. FPS Finance
 - b. CFI
 - c. FPS Economy

Hoofdstuk 5

1. Ben ik wettelijk verplicht om verdachte transacties te melden aan de CFI?
 - a. Ja. Ik ben verplicht dit te doen en geniet immuniteit — er bestaat geen risico op vervolging
 - b. Nee. Melden is vrijwillig
 - c. Ja, maar enkel voor transacties boven een bepaald bedrag of afkomstig uit bepaalde landen
 - d. Ja, maar enkel indien ik zeker ben dat er sprake is van witwassen

Hoofdstuk 6

1. Een AML-controle wordt vooraf aangekondigd zodat u tijd heeft om uw dossiers voor te bereiden.
 - a. Juist
 - b. Onjuist
2. Tijdens een AML-controle selecteert de inspecteur een aantal tegenpartijdossiers om te controleren. Hoeveel dossiers worden doorgaans geselecteerd en hoe ver kunnen deze teruggaan?
 - a. 5 tot 10 dossiers, tot 1 jaar terug
 - b. 20 tot 30 dossiers, tot 3 jaar terug
 - c. 50 tot 100 dossiers, tot 5 jaar terug
 - d. Alle dossiers van het afgelopen jaar
3. De AML-verantwoordelijke is niet beschikbaar op de dag van een controle. Wat gebeurt er?
 - a. De controle wordt automatisch uitgesteld totdat de AML-verantwoordelijke aanwezig is
 - b. De controle kan niet doorgaan — enkel de AML-verantwoordelijke is wettelijk bevoegd om te antwoorden
 - c. Een andere werknemer moet de rol kunnen overnemen en de inspecteur de gevraagde informatie kunnen bezorgen
 - d. De onderneming kan de documenten binnen de 5 werkdagen per e-mail bezorgen
4. Welke van de volgende zaken kan een inspecteur NIET vragen tijdens een AML-controle?
 - a. U vragen uit te leggen waarom u een specifieke tegenpartij hebt aanvaard
 - b. Uw AML-certificaat voorleggen
 - c. Aantonen dat u verdachte transacties aan de CFI hebt gemeld wanneer vereist
 - d. Een lijst bezorgen van alle transacties boven €1.000 van de afgelopen 10 jaar

Annex A – Risk scorecard: general risk assessment on company level and actions to be taken

	The director(s) of the diamond trader has/have blank criminal record.	
	The diamond trader recently had an inspection by the FPS Economy concerning the implementation of the anti-money laundering law in his company, without any consequences.	Feedback about the inspection can be obtained at the FPS Economy.
	The diamond trader always does a notification to the CFI when he encounters a suspicious transaction or fact which could possibly relate to ML/FT.	CFI contact details: Email: info@ctif-cfi.be of Tel. 02 533 72 11
	The diamond trader applies the recommendations from the AWDC ' <i>Best practice guide for trade in the Belgian diamond sector</i> '.	
	The diamond trader complies with this anti-money laundering policy.	
	The diamond trader uses the KYCP platform.	The diamond trader can demonstrate this on the basis of the list of onboarded clients/suppliers in KYCP
	The diamond trader applies the recommendations in the AWDC guide ' <i>Sanctions and embargoes compliance guide for the diamond trade</i> '.	
	The diamond trader is part of a group and all entities of the group apply a similar anti-money laundering policy.	
	The diamond trader annually has many new clients/suppliers and/or a client/supplier portfolio that changes regularly.	
	One or more directors of the diamond trader have had a bankruptcy in the past.	
	The diamond trader regularly does business with countries with less supervision on the banking industry and/or a favorable fiscal regime / or countries with high risk on ML/TF	Check the following links for information about countries: https://index.baselgovernance.org/ https://www.transparency.org/cpi2018 http://www.fatf-gafi.org/countries/#high-risk https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/
	The diamond trader regularly has discussions at Diamond Office about the value of his imported or exported goods.	
	The diamond trader regularly receives or does money transfers from or to countries with less supervision on the banking industry and/or a favorable fiscal regime.	
	A part of the client/supplier portfolio of the diamond trader refuses to provide identification information and documentation about themselves/their company.	

	The diamond trader regularly receives or does payments (related to diamond transactions) in cash in countries where there are no or limited cash limits.	
	The diamond trader has a complex or untransparent company structure.	
	The diamond trader sells diamonds through the internet or through online platforms.	
	The diamond trader regularly does business with countries to which sanctions or embargoes apply and/or countries which are not member of the Kimberley Process.	The diamond trader follows the '<i>Sanctions and embargoes compliance guide for the diamond trade</i>' and assesses whether, despite the high risk, it is nonetheless possible to do business, in case certain risk mitigating measures are taken. http://www.fatf-gafi.org/countries/#high-risk https://www.transparency.org/cpi2018 https://www.kimberleyprocess.com/en/kp-participants-and-observers
	The diamond trader is not registered at the FPS Economy, or his registration was suspended or cancelled.	

Annex B – Risk scorecard for accepting individual client or supplier relationships and actions to be taken

	No risks were detected via the GRID screening tool in the KYCP platform.	
	The counterparty understands the anti-money laundering legislation or similar legislation in his country and actively cooperates to provide the diamond trader all required information.	
	The counterparty is located in a EU member state, or a country outside of the EU with an effective anti-money laundering regime.	
	The diamond trader received positive references about the counterparty.	
	The counterparty is RJC (Responsible Jewellery Council) certified.	https://www.responsiblejewellery.com/members/
	The counterparty is member of a recognized diamond bourse.	The diamond trader asks for the bourse membership card.
	The counterparty is resident of a country with less supervision on the banking sector and/or a favorable fiscal regime and/or a country with a failing anti-money laundering regime/ a conflict affected and high risk area	The diamond trader undertakes the following: - obtains permission of the senior management staff in his company to conclude the business relationship and/or to execute the transaction; - gathers information about the client and its ultimate beneficial owner(s), about the intended nature of the business relationship, about the source of the funds used and the source of the client's wealth and that of its ultimate beneficial owner(s), about the reasons for the intended transactions or the executed transactions; - enhances his supervision of the business relationship;

	The counterparty has or seems to have little experience in the diamond sector.	The diamond trader asks the counterparty what kind of business relationship of or sort of occasional transaction he intends to have
	The counterparty works through one or several intermediary(ies) and/or the diamond trader has never met the client personally and it is also not clear which role the intermediary(ies) play(s) exactly.	- The diamond trader insists on meeting the counterparty personally and asks for clarification about the involvement of the different parties. - If the counterparty is a high-net-worth individual (HNWI, a person with large capital), the diamond traders asks a bank statement of this person.
	The diamond trader has had bad experiences with the client in the past (suspicion of money laundering, financing of terrorism).	
	The counterparty went bankrupt in the past and recently established a new company.	The diamond trader asks for the reasons of the previous bankruptcy.
	The counterparty is located in a country which is not a member of the Kimberley Process.	https://www.kimberleyprocess.com/en/kp-participants-and-observers The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty requests you not to analyze his identity, insist on anonymity, and/or is prepared to pay/compensate for this.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty is/was persecuted for certain serious crimes, such as money laundering, financing of terrorism, fraud.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty is on a sanction list.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.
	The counterparty is a Belgian diamond trader/broker not registered at the FPS Economy.	The diamond trader does not enter into the business relationship or does not execute the occasional transaction and notifies the CFI.

		• makes sure that at least the first transaction is executed via an account on the client's name with a credit institution where the vigilance measures towards clients are not less strict than the principles established as per the anti-money laundering law. The source of the funds can possibly be checked by asking confirmation to the client that his financial resources stem from the ordinary operating funds of the company. Also pay checks, tax declaration documents, independent audit reports or media reports could provide information on this. Check the following links for information about countries: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing/eu-policy-high-risk-third-countries_en https://index.baselgovernance.org/ https://www.transparency.org/cpi2018 http://www.fatf-gafi.org/countries/#high-risk https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/ https://www.cahraslist.net/cahras
	The ownership structure of the company of the counterparty seems unusually or excessively complex considering the type of company activity.	The diamond trader requests to provide a clear structure or organizational chart of the company, if applicable with the shareholder registers or other pieces of evidence which can demonstrate the identity of the ultimate beneficiaries.
	The diamond trader never met his counterparty personally.	
	Negative media is connected to the counterparty	
	The counterparty is a politically exposed person (PEP), family member of a PEP or close associate of a PEP.	The diamond trader takes extra vigilance measures for clients who are PEPs, family members of close associates thereof. In any case he takes the following measures: - o He obtains permission of the higher management in the company to enter into or continue the business relationship with these persons; - o He takes appropriate measures to determine the origin of the funds which are used in the business relationship or transactions with these persons; - o He exercises a stricter supervision on the business relationship and the execution of the transaction.
	The identification details which the counterparty has provided, do not correspond to information which one finds through certain verification tools.	The diamond trader asks additional documents to verify the identity of his client or supplier.
	The identification details which the counterparty provided, are not official, do not look authentic or are not up-to-date.	The diamond trader asks additional documents to verify the identity of his client or supplier.
	It is unclear what type of business relationship/occasional transaction the counterparty wants.	The diamond trader asks the counterparty what kind of business relationship of or sort of occasional transaction he intends to have.
	The counterparty is active in a sector where the purchase or sale of diamonds does not logically fit in its corporate purpose (e.g. a sector other than diamond trade, jewelry,...)	The diamond trader pays attention if the sector in which the counterparty is active is a high-risk sector such as second-handed vehicles, construction, ...

Annex C – Risk scorecard for monitoring during business or occasional relationship

	The counterparty executes payments and/or invoices in accordance with the AWDC ' <i>Best practice guide for trade in the Belgian Diamond sector</i> '.	Where appropriate, the diamond trader insists with the counterparty to follow the recommendations in this guide.
	The flow of goods which relate to transactions with a counterparty outside of the European Union are being controlled by the Belgian Diamond Office.	This is a legal obligation
	The counterparty pays from a country with less supervision on the banking sector and/or a favorable fiscal regime and/or with a high money laundering and/or corruption risk and/or countries for which sanctions/embargoes apply and/or countries which are not member of the Kimberley Process.	The diamond trader will monitor these transactions even more closely, check the origin of the funds and see whether these are consistent with the individual risk analysis made of the client.
	The seller's invoice does not clearly indicate whether it concerns synthetic/treated diamonds or (natural) diamonds.	The diamond trader follows the recommendations of the AWDC ' <i>Best practice guide for trade in the Belgian diamond sector</i> '.
	The counterparty often changes his bank account.	The diamond trader asks his counterparty to explain.
	The client wants to pay through a currency broker, money transfer services (MoneyGram), Hawala or payments in new digital coins (e.g. Bitcoin).	The diamond trader follows the recommendations of the AWDC ' <i>Best practice guide for trade in the Belgian diamond sector</i> '.
	The counterparty suggests an atypical payment/delivery method (e.g. payment through a third party, payment through the account of a third party, payment through other channels than official banks/financial institutions is proposed).	The diamond trader asks the counterparty to explain. He checks the origin of the funds and whether these are consistent with the individual risk analysis made of the client. Where appropriate, he makes a tripartite agreement as recommended in the AWDC ' <i>Best practice guide for trade in the Belgian diamond sector</i> '.
	The counterparty wants to execute a complex or unconventionally big transaction with does not have a visible economic or legitimate purpose.	The diamond trader checks the origin of the funds and whether these are consistent with the individual risk analysis made of the counterparty. He asks his counterparty to explain and follows the recommendations of the AWDC ' <i>Best practice guide for trade in the Belgian diamond sector</i> '.
	The client insists on cash payments of more than 3,000 Euros in Belgium.	The diamond trader does not execute the transaction and notifies the CFI.
	The supplier of the diamond trader cannot provide a Kimberley Process Certificate for the delivery of rough diamonds or it concerns a rough transaction from a country that is not member of the Kimberley Process.	The diamond trader does not execute the transaction and notifies the CFI.

TOOLS TO HELP COMPLY WITH AML

AWDC

KYCP

Identifying & verifying counterparties

Risk assessment

Updating AML information

Screening tool access: ORBIS & GRID

MYAWDC

Watch AML seminar + acquire AML certificate

Watch Best Practices seminar + acquire Best Practices certificate

Consult invoices

Consult G7 & GF certificates

Consult customs documents & track shipments

QUESTIONS?

CONTACT AWDC HELPDESK

Tuesday, Wednesday & Thursday (10am - 1pm)
compliance@awdc.be

FPS ECONOMY

DIAMOND SUPERVISION

Submit AML report

Consult previous AML reports

Submit stock declaration

Consult public list of registered diamond companies

Submit KP declarations

QUESTIONS?

CONTACT FPS ECONOMY



diamond@economie.fgov.be



02 277 54 59

Organisational Obligations

Have internal AML policy
Appoint min. 1 AML officer
Pass online AML quiz yearly or physical
AML exam 3-yearly
Submit annual AML report to FPS
Economy

Risk Analysis

Based on KYC, assess safety of doing
business with this party
Use risk scorecards to assign
risk category (low, medium, high)
Keep info up-to-date

Reporting Suspicious Situations

Identify suspicious situations
Report unusual of suspicious actions, even
without proof, to CFTI
Protect your company and contribute to
reputation of Antwerp's diamonds

The AML Journey

1

2

3

4

5

KYC (Know Your Counterparty)

Collect AML related info about
counterparty before establishing
relationship
Verify, keep up-to-date, and store properly
→ Know who you're doing business with
to manage risks

Make a Decision

Accept the business relationship
OR
Accept under certain conditions
OR
Refuse or terminate the business
relationship