Bereik aantoonbare risicobeheersing met een effectieve SIRA

Een praktisch 5-stappenplan in lijn met de DNB Good Practices SIRA (2025)

Nederlands compliance Instituut
sinds 1999

Inleiding

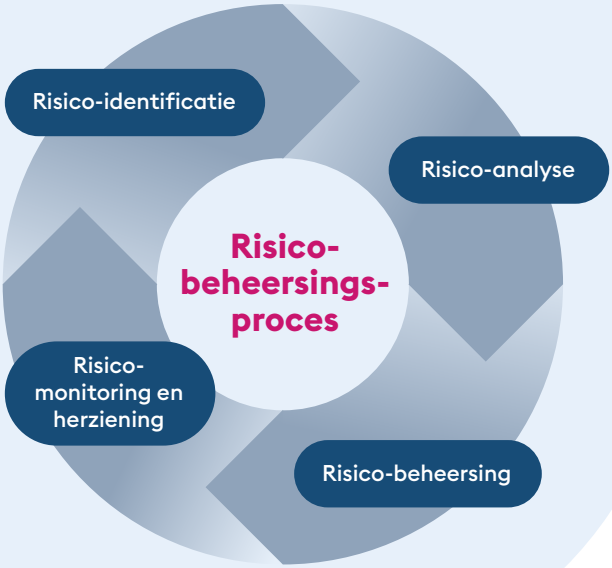
Integriteitsrisico's vormen een structureel aandachtspunt voor financiële instellingen. Banken, verzekeraars, betaalinstellingen en andere onder toezicht staande ondernemingen worden geconfronteerd met risico's zoals witwassen, fraude, sanctieontwijking en andere vormen van financiële criminaliteit. Deze risico's kunnen niet alleen leiden tot financiële schade, maar raken ook het vertrouwen in de financiële sector en de integriteit van het financiële stelsel.

Om deze risico's systematisch te beheersen, zijn instellingen verplicht een systematische integriteitsrisicoanalyse (SIRA) uit te voeren. Voor financiële ondernemingen volgt deze verplichting onder meer uit artikel 3:10 Wft in samenhang met artikel 10 Besluit prudentiële regels Wft, terwijl voor Wwft-instellingen de verplichting is verankerd in artikel 2b en 2c Wwft.

De Nederlandsche Bank (DNB) heeft de invulling van deze verplichting nader toegelicht in onder meer de Good Practices SIRA (2025). Deze publicatie beschrijft hoe instellingen hun integriteitsrisico's systematisch kunnen identificeren, analyseren, beheersen en monitoren.

De kern van deze benadering is dat een SIRA geen statisch document is, maar een dynamisch instrument voor risicobeheersing. Een effectieve SIRA maakt zichtbaar welke integriteitsrisico's een organisatie loopt, hoe deze worden beoordeeld en hoe beheersmaatregelen bijdragen aan het reduceren van het inherente risico tot een restrisico dat past binnen de vastgestelde risicobereidheid.

De DNB Good Practices beschrijven daarbij een cyclisch proces van risico-identificatie, analyse, beheersing en monitoring. Het in dit document beschreven 5-stappenplan vormt een praktische vertaling van deze cyclus en biedt organisaties een werkbare methodiek om hun integriteitsrisicoanalyse gestructureerd in te richten.



Aanleiding

Hoewel vrijwel alle instellingen formeel een SIRA hebben opgesteld, blijkt in de praktijk dat de kwaliteit en toepasbaarheid sterk kunnen verschillen. Tijdens toezichtonderzoeken blijkt regelmatig dat organisaties moeite hebben om toe te lichten waarom bepaalde risico's als hoog of laag zijn geclassificeerd, hoe risicoscores tot stand zijn gekomen en hoe specifieke beheersmaatregelen bijdragen aan het reduceren van het risico.

Wanneer deze onderbouwing ontbreekt, verschuift het gesprek met bestuur of toezichthouder al snel van risicobeheersing naar het verdedigen van aannames. De SIRA verliest daarmee haar waarde als sturingsinstrument. Daarnaast bestaat in veel organisaties het risico van een zogenoemde checkboxbenadering. Risico's worden benoemd, maar niet geprioriteerd. Maatregelen worden beschreven zonder duidelijke koppeling aan specifieke risico's. Monitoring vindt plaats zonder duidelijke indicatoren of escalatiemechanismen.

Toezichthouders verwachten echter dat instellingen hun integriteitsrisico's systematisch identificeren, analyseren en beheersen en dat zij hun keuzes consistent, reproduceerbaar en goed onderbouwd kunnen toelichten. Een professionele SIRA moet daarom niet alleen logisch zijn opgebouwd, maar ook navolgbaar, toetsbaar en bestuurlijk verdedigbaar.

Een gestructureerde methodiek helpt organisaties om deze verwachtingen te vertalen naar een praktisch werkbaar proces. Het hier beschreven vijf-stappenplan sluit aan bij de systematiek van de DNB good practices en biedt een praktische aanpak om integriteitsrisico's aantoonbaar te beheersen.

Het 5-stappenplan voor een effectieve SIRA

Stap 1

Bepaal de scope en het organisatierisicoprofiel

Een effectieve SIRA begint met het vaststellen van de context waarin de organisatie opereert. In deze eerste stap wordt het normatieve kader vastgesteld, wordt de organisatorische scope afgebakend en wordt het organisatierisicoprofiel opgesteld.

Het normatieve kader omvat de externe en interne normen die richting geven aan de risicoanalyse. Denk hierbij aan relevante integriteitswetgeving, zoals de Wwft en bepalingen uit de Wft en onderliggende regelgeving. Daarnaast spelen toezichthouderpublicaties, waaronder guidance en good practices van DNB, een belangrijke rol bij de interpretatie van open normen. Ook interne beleidsdocumenten en gedragscodes maken onderdeel uit van dit kader.

Vervolgens wordt de organisatorische scope van de SIRA bepaald. Daarbij wordt expliciet beschreven welke rechtspersonen, producten en diensten, klantgroepen, geografische markten, distributiekanalen en transactiestromen binnen de analyse vallen. Door deze afbakening duidelijk vast te leggen wordt voorkomen dat impliciete aannames ontstaan en wordt de reproduceerbaarheid van de analyse vergroot.

Op basis van deze context wordt een organisatierisicoprofiel opgesteld. Hierin worden kenmerken beschreven die bepalend zijn voor de aard en intensiteit van integriteitsrisico's, zoals de omvang en complexiteit van de organisatie, strategische plannen en relevante externe ontwikkelingen.

Tot slot wordt in deze fase de risicobereidheid vastgesteld. Het bestuur bepaalt welk restrisico acceptabel wordt geacht in het licht van strategie, maatschappelijke positie en toezichtverwachtingen. Deze risicobereidheid vormt later het referentiepunt bij de beoordeling van restrisico's.

Stap 2

Identificeer relevante integriteitsrisico's

Wanneer de context duidelijk is, kan de organisatie systematisch bepalen welke integriteitsrisico's relevant zijn. Het doel van deze stap is niet het samenstellen van een theoretische lijst van mogelijke risico's, maar het identificeren van risico's die daadwerkelijk voortvloeien uit de kenmerken van de organisatie.

Een praktische manier om risico's te identificeren is het analyseren van zogenoemde risicodrivers. Daarbij wordt gekeken naar factoren zoals cliënten en klantgroepen, producten en diensten, transactiestromen, distributiekanalen en geografische blootstelling. Deze factoren moeten niet afzonderlijk worden beoordeeld, maar juist in samenhang worden beschouwd.

Risico's worden bij voorkeur geformuleerd in concrete risicoscenario's. In plaats van een abstracte beschrijving van een witwasrisico wordt het risico bijvoorbeeld omschreven als het scenario waarin via een bepaald product, aangeboden aan een specifieke klantgroep in een bepaalde regio, ongebruikelijke transacties onopgemerkt blijven.

Bij elk risico wordt onderscheid gemaakt tussen externe dreigingen en interne kwetsbaarheden. Externe dreigingen kunnen bijvoorbeeld bestaan uit witwasconstructies of fraudepraktijken, terwijl interne kwetsbaarheden kunnen voortkomen uit productcomplexiteit, afhankelijkheid van handmatige controles of beperkte automatisering.

Door dit onderscheid wordt duidelijk waar het risico ontstaat en waar beheersmaatregelen effectief kunnen worden ingezet.

Stap 3

Beoordeel en onderbouw de risico's

Na identificatie van de relevante risico's volgt de systematische risicobeoordeling. In deze fase wordt vastgesteld hoe groot het inherente risico is: de kans dat een risico zich voordoet en de impact die dat zou hebben, zonder rekening te houden met bestaande beheersmaatregelen.

De beoordeling gebeurt doorgaans aan de hand van een kans-impactbenadering. Het is daarbij belangrijk dat definities van kans en impact vooraf duidelijk worden vastgelegd en dat beoordelingscriteria concreet en toepasbaar zijn. Alleen dan kunnen verschillende beoordelaars tot vergelijkbare scores komen en wordt de methodiek reproduceerbaar.
De impact van integriteitsrisico's kan vanuit verschillende perspectieven worden bekeken, bijvoorbeeld financieel, juridisch-regulatoir, reputatiegerelateerd of vanuit de continuïteit van de onderneming.

Minstens zo belangrijk als de score zelf is de onderbouwing ervan.
Per risico moet duidelijk worden vastgelegd waarom een bepaalde kans- of impactscore is toegekend en welke aannames daarbij zijn gehanteerd. Toezichthouders kijken nadrukkelijk naar deze redenering en toetsen of vergelijkbare risico's consistent zijn beoordeeld.

Stap 4

Koppel maatregelen en bepaal het restrisico

In de vierde stap wordt bepaald hoe de organisatie de geïdentificeerde risico's beheerst. Per materieel risico worden bestaande beheersmaatregelen in kaart gebracht en expliciet gekoppeld aan het betreffende risico.

Het is belangrijk dat maatregelen niet generiek worden beschreven, maar concreet worden gekoppeld aan specifieke risico's. Daarbij wordt vastgelegd welke maatregel wordt toegepast, welk risico hiermee wordt gemitigeerd en wie verantwoordelijk is voor uitvoering.
Vervolgens wordt beoordeeld hoe effectief deze maatregelen zijn.

Daarbij wordt niet alleen gekeken naar het ontwerp van de maatregel, maar ook naar de werking in de praktijk. Een maatregel kan op papier adequaat zijn, maar in de praktijk onvoldoende effect hebben wanneer zij niet consistent wordt uitgevoerd.

Op basis van deze beoordeling wordt het restrisico vastgesteld: het risico dat overblijft nadat de maatregelen zijn toegepast. Dit restrisico wordt vervolgens getoetst aan de eerder vastgestelde risicobereidheid.
Wanneer het restrisico hoger is dan acceptabel wordt geacht, moeten aanvullende maatregelen worden overwogen of moet een expliciete bestuurlijke afweging plaatsvinden.

Stap 5

Monitor, herijk en borg de SIRA in governance

De laatste stap zorgt ervoor dat de SIRA geen eenmalige analyse blijft, maar een continu onderdeel wordt van het risicomanagementproces.

Per materieel risico wordt vastgesteld welke indicatoren inzicht geven in de werking van beheersmaatregelen en mogelijke veranderingen in het risicoprofiel. Dit kunnen bijvoorbeeld trends in ongebruikelijke transacties, auditbevindingen, incidentmeldingen of signalen vanuit toezicht zijn.

Daarnaast worden drempelwaarden en escalatiemechanismen vastgesteld. Wanneer bepaalde signalen een vooraf bepaalde grens overschrijden, moet duidelijk zijn hoe escalatie plaatsvindt en wie verantwoordelijk is voor besluitvorming.
Naast doorlopende monitoring wordt de SIRA periodiek herijkt en opnieuw beoordeeld wanneer materiële wijzigingen optreden, bijvoorbeeld bij nieuwe producten, uitbreiding naar nieuwe markten, significante incidenten of relevante wetswijzigingen.

Bestuurlijke betrokkenheid is hierbij essentieel. Het bestuur stelt de SIRA formeel vast, bespreekt periodieke rapportages en neemt expliciet besluiten over restrisico's en eventuele aanvullende maatregelen.

Tot slot wat je nu hebt

Wanneer de vijf stappen zorgvuldig zijn doorlopen, beschikt de organisatie over een systematisch opgebouwde en bestuurlijk verankerde integriteitsrisicoanalyse. De context en scope zijn expliciet vastgelegd, het organisatierisicoprofiel is helder beschreven en materiële risico's zijn herleidbaar geïdentificeerd.

De risicobeoordeling is onderbouwd en reproduceerbaar, beheersmaatregelen zijn aantoonbaar gekoppeld aan concrete risico's en het restrisico is expliciet getoetst aan de vastgestelde risicobereidheid. Monitoring, escalatie en periodieke herijking zijn ingericht als onderdeel van de governance-cyclus. Daarmee is de SIRA niet slechts een document, maar een sturingsinstrument dat inzicht geeft in risicoprioriteiten, besluitvorming ondersteunt en toezichtgesprekken inhoudelijk versterkt. Aantoonbare risicobeheersing betekent in dit kader niet dat risico's worden uitgesloten, maar dat zij bewust worden gewogen, proportioneel worden beheerst en bestuurlijk worden gedragen.

Volgende stap

Het opstellen van een methodisch correcte SIRA is één stap. Het consequent toepassen, herijken en verbeteren ervan vraagt om inhoudelijke scherpte en praktijkervaring. In veel organisaties blijkt juist de vertaling van analyse naar bestuurlijke besluitvorming en operationele uitvoering de grootste uitdaging.

Voor professionals die deze systematiek niet alleen willen begrijpen, maar ook willen toepassen op realistische casuïstiek en actuele toezichtontwikkelingen, biedt verdere verdieping meerwaarde. Het Werkcollege SIRA van het Nederlands Compliance Instituut is hiervoor een uitstekend middel. Het Werkcollege SIRA is ontwikkeld om deze vertaalslag te ondersteunen, met aandacht voor scenario-denken, consistent scoren, effectiviteitsbeoordeling van maatregelen en bestuurlijke verankering.

Voor wie is het Werkcollege SIRA?

Het werkcollege is voor compliance professionals die verantwoordelijk zijn voor de inrichting, begeleiding of toetsing van het SIRA-proces. Dat kunnen ervaren tweedelijns professionals zijn, maar ook functionarissen die compliance als aanvullende verantwoordelijkheid hebben gekregen.

Wat kan je verwachten?

Deelnemers zijn met name professionals die niet alleen een SIRA willen “opleveren”, maar die het proces zodanig willen structureren dat het consistent, juridisch houdbaar, inhoudelijk uitlegbaar, bestuurlijk verdedigbaar én reproduceerbaar is. Het werkcollege ondersteunt compliance professionals bij het structureren van dit proces, zodat de SIRA niet slechts een document is, maar een onderbouwd en aantoonbaar werkend sturingsinstrument.

Breng je SIRA naar het volgende niveau met dit hands-on werkcollege: van risk appetite en inherent/residueel risico tot evidence-based control-beoordeling. We werken met actuele DNB Good Practices (2025) en de EBA-risicofactoren, zodat je met direct toepasbare kennis en handvatten de deur uitgaat.

Docent is Peter Westdijk, senior compliance & privacy officer bij NCIP. De sessie vergt een actieve bijdrage en inzet van de deelnemers.

Meer informatie of direct inschrijven? Bekijk daarvoor deze pagina.

Meer informatie

Waarom NCI?

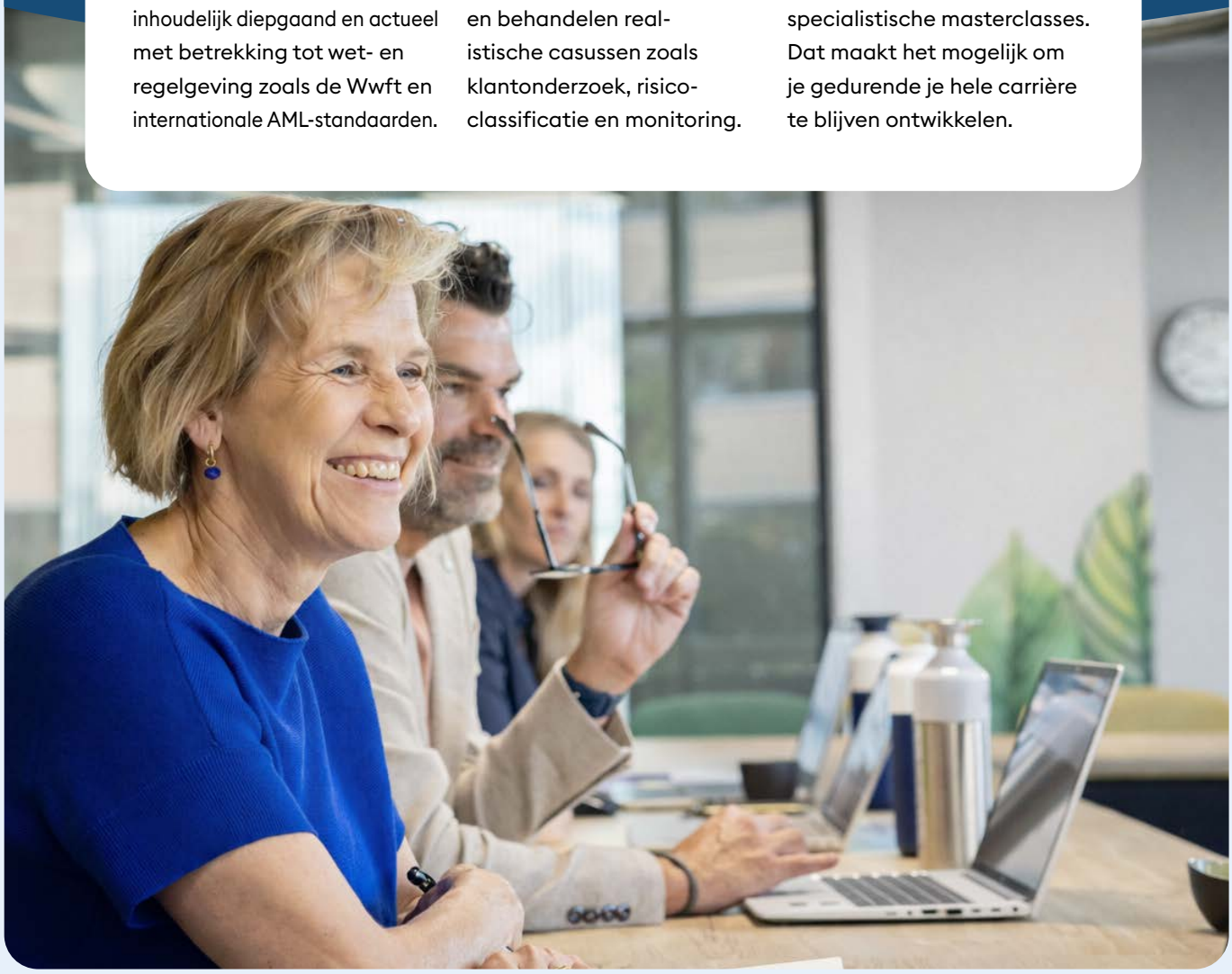
Het Nederlands Compliance Instituut (NCI) wordt in Nederland vaak gezien als een van de meest gespecialiseerde opleiders op het gebied van compliance, integriteit en AML/CDD. Hun programma's zijn specifiek gericht op professionals in de financiële sector en bieden zowel leergangen als specialistische modules.

3 redenen waarom professionals voor NCI kiezen

Sterke specialisatie in compliance en integriteit
NCI richt zich volledig op compliance, integriteit en financiële criminaliteit. Daardoor zijn de opleidingen inhoudelijk diepgaand en actueel met betrekking tot wet- en regelgeving zoals de Wwft en internationale AML-standaarden.

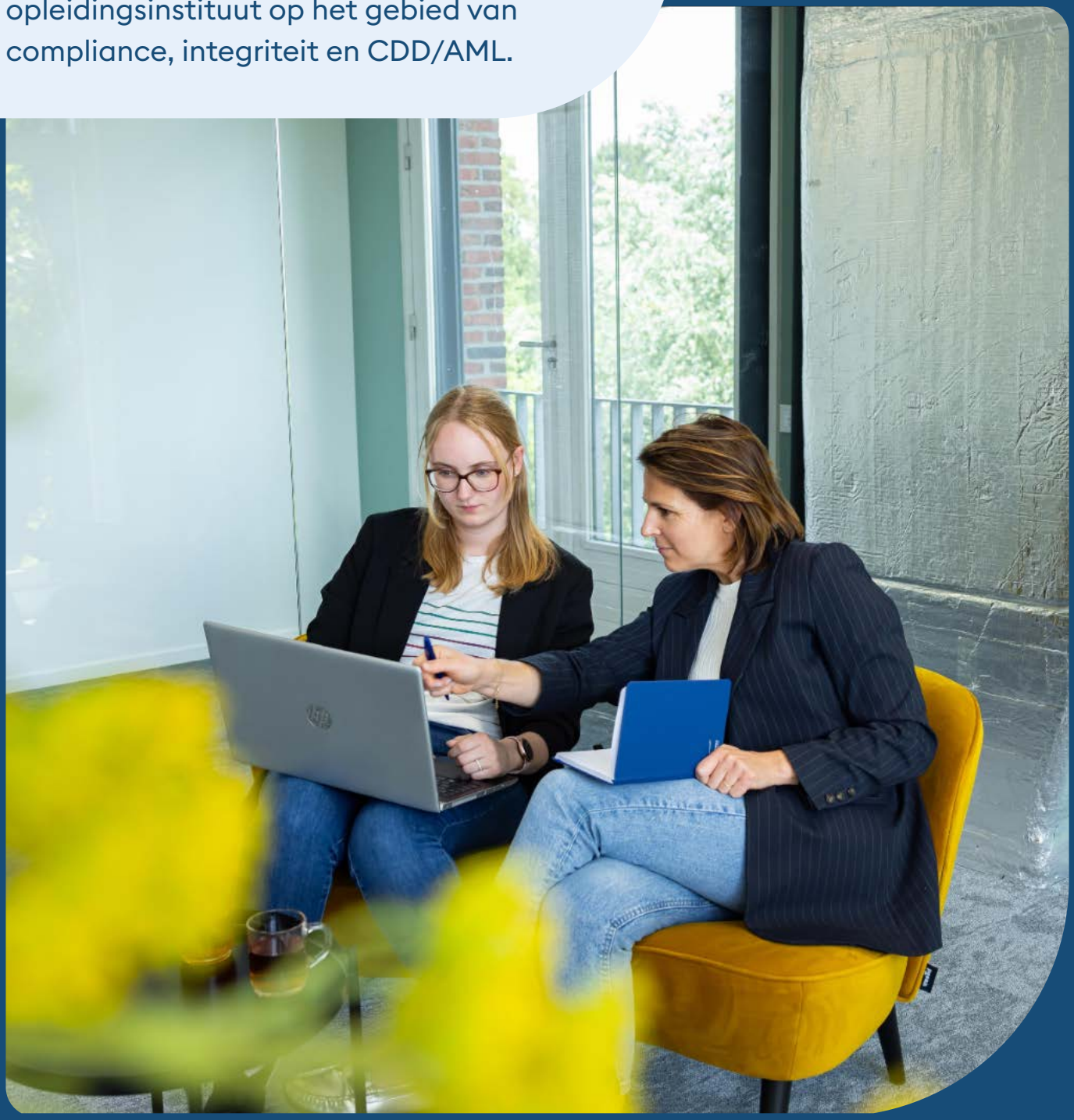
Praktijkgerichte opleidingen met experts uit het vakgebied
Opleidingen worden gegeven door ervaren compliance-professionals en behandelen realistische casussen zoals klantonderzoek, risicoclassificatie en monitoring.

Breed aanbod voor verschillende rollen en ervaringsniveaus
Van basistraining AML/CDD tot leergangen voor compliance officers en specialistische masterclasses. Dat maakt het mogelijk om je gedurende je hele carrière te blijven ontwikkelen.



Over NCI

Het Nederlands Compliance Instituut bestaat sinds 1999 en is een toonaangevend opleidingsinstituut op het gebied van compliance, integriteit en CDD/AML.



Vind ons op:

www.compliance-instituut.nl

Wij zijn bereikbaar via
info@compliance-instituut.nl
of via 010-3032548.