RAPPORT ANALYSE

SREP Marktbeeld 2025

In het kort - in het kader van het Supervisory Review and Evaluation Proces (SREP) stuurt de AFM periodiek een vragenlijst naar beleggingsondernemingen. Het betreft zowel vermogensbeheerders als beheerders van beleggingsinstellingen met een MiFID-top up als Handelaren voor Eigen Rekening (HER's) en handelsplatformen. Het betreft in totaal 239 partijen. In dit SREP Marktbeeld geven we een terugkoppeling gebaseerd op de evaluatie van de response op de vragenlijst uit het najaar van 2025. Aan de hand van deze terugkoppeling kunt u nagaan waar uw bedrijfsvoering nog ruimte biedt voor verbetering.

JUNI | 2026

AFM

Samenvatting

Het Supervisory Review and Evaluation Proces (SREP) vloeit voort uit IFR/IFD en de EBA- en ESMA-richtsnoeren en verplicht Europese toezichthouders periodiek een integraal risicobeeld van beleggingsondernemingen op te stellen. In het Nederlandse twin-peaks model richt de SREP-uitvraag van de AFM zich specifiek op het bedrijfsmodel en op een beheerste en integere bedrijfsvoering. Het SREP combineert kwantitatieve indicatoren, zoals incidenten, klachten, ontwikkeling klantenbestand en toevertrouwd vermogen, met een jaarlijkse selectie van inhoudelijke thema's.

De AFM richt zich bij de SREP uitvragen op de onderdelen die de beheerste en integere bedrijfsvoering betreffen. Dit domein is echter breed. De AFM kiest er dan ook voor om de verschillende onderdelen zoals risicobeheer, uitbesteding, beloningsbeleid, leiderschap & cultuur gefaseerd uit te vragen. De uitslagen worden omgezet in zogenaamde SREP-scores. SREP werkt met een doorlopende normering van 1 tot 4 waarbij een 1 staat voor een sterke beheersing en een 4 duidt op een inadequate beheersing van het betreffende risico. Binnen deze systematiek staat 2 voor adequaat en 3 voor zwak. De geaggregeerde resultaten kunnen meegenomen worden voor risicosignalering en (thematische) onderzoeken op sector en/of segmentniveau.

In het najaar van 2025 stonden zeven thema's centraal: implementatie van wet- en regelgeving, vakbekwaamheid, best execution, duurzaamheid, interne controle, IT-risicobeheersing en klantbediening met inzet van derden. De uitkomsten laten een wisselend beeld zien. Positief is dat veel ondernemingen hun voorbereiding op nieuwe regelgeving, vakbekwaamheidsevaluaties en de opzet van de compliance functie grotendeels op orde hebben.

Tegelijkertijd blijken de werking en volwassenheid van interne controles, de structurele borging van best execution, de vastlegging en integratie van duurzaamheidsrisico's en de beheersing van IT-risico's regelmatig tekort te schieten. Ook de inzet van derden vraagt blijvende aandacht, gezien de impact op het verdienmodel, de kwaliteit van dienstverlening en de duidelijkheid richting klanten over verantwoordelijkheden en aansprakelijkheid. Op IT-gebied zijn er met name zwaktes te zien bij vulnerability management, business continuity en hersteltesten.

Ongeveer een kwart van de ondernemingen heeft naar aanleiding van eerdere SREP-uitvragen al concrete verbetermaatregelen doorgevoerd, vooral in beleid, processen en interne beheersing. De AFM verwacht dat marktpartijen de observaties uit dit SREP-marktbeeld benutten om hun bedrijfsvoering kritisch te herijken en waar nodig verder te versterken.

In september 2026 komt onze volgende SREP-uitvraag. U wordt daar nog uitgebreid over geïnformeerd. Naast een aantal terugkerende vragen die bijdragen aan het beeld van de bedrijfsvoering zullen we dit jaar onder andere stil staan bij het Product Approval & Review Proces (PARP), modelrisico's, belangenverstrengeling, financiële inclusie en inrichting bestuur & management. Een paar weken voor dat de vragenlijst ter beantwoording open wordt gezet in het AFM Portaal ontvang u de aankondigingsbrief en ter voorbereiding een pdf van de vragenlijst.

Inhoudsopgave

1. Implementatie wet- en regelgeving

1.1 Voorkomen is beter dan genezen

Een goede en volledige verwerking van nieuwe of gewijzigde wet- en regelgeving in beleid, procedures en processen geeft een indicatie van de beheerste en integere bedrijfsvoering.
Daarnaast is het een indicatie van het effectief functioneren van de compliancefunctie en mate van compliancegerichtheid. Om deze redenen is de voorbereiding op en implementatie van wet- en regelgeving opgenomen in deze SREP-uitvraag.

1.2 Voorbereiding regelgeving over het algemeen op orde

De voorbereiding op de implementatie van nieuwe en gewijzigde wet- en regelgeving is over het algemeen goed op orde. Ruim 80% van de ondernemingen heeft dit thema adequaat tot goed beheerst. Een belangrijke succesfactor daarbij is een goed toegeruste compliancefunctie, met voldoende middelen, kennis en capaciteit om de implementatie van regelgeving te begeleiden en te monitoren.

Op basis van de antwoorden identificeert de AFM de volgende good practices:

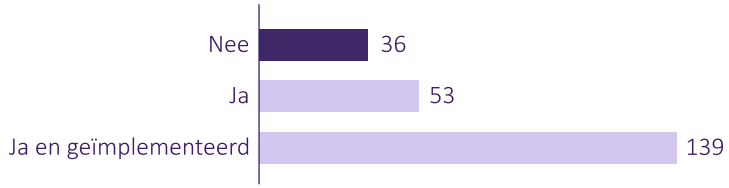
- werken met een gestandaardiseerde en gestructureerde projectaanpak
- wijzigingen systematisch verwerken in beleid, procedures en processen
- nieuwe regelgeving opnemen in het compliance-monitoringsplan en dit monitoren
- verantwoordelijkheden en bevoegdheden duidelijk vastleggen
- meerdere disciplines betrekken bij de implementatie
- structureel budget beschikbaar stellen
- ontwikkelingen in wet- en regelgeving doorlopend in kaart brengen
- meerdere informatiebronnen raadplegen om ontwikkelingen te volgen

De meeste ondernemingen raadplegen vijf of meer bronnen om relevante ontwikkelingen bij te houden. Nationale toezichthouders, externe adviseurs en de pers worden daarbij het meest genoemd.

1.3 Aandachtspunten

De belangrijkste redenen voor een zwakke(re) score op dit domein lijkt gekoppeld aan het ontbreken van het documenteren van verantwoordelijkheid binnen de organisatie voor implementatie van wet- en regelgeving en het ontbreken van een gestandaardiseerde projectaanpak bij dergelijke trajecten.

Figuur 1.1 Antwoordverdeling gestandaardiseerde projectaanpak



Beschikt uw onderneming over gestandaardiseerde (project)aanpak voor het monitoren en implementeren van nieuwe wet- en regelgeving?

2. Vakbekwaam

2.1 Regels voor medewerkers die informeren of adviseren over beleggen

Beleggingsondernemingen moeten ervoor zorgen dat medewerkers die informeren of adviseren over beleggen beschikken over de juiste vakbekwaamheid om hun verantwoordelijkheden goed te kunnen vervullen. Dat staat in artikel 4.9 van de Wet op het Financieel Toezicht (Wft). Dit is een doorlopende verplichting.

De precieze vakbekwaamheidsvereisten zijn opgenomen in artikel 2 van de Regeling vakbekwaamheid werknemers beleggingsondernemingen Wft (Regeling vakbekwaamheid). Medewerkers die mogen adviseren over beleggen, mogen ook informeren over beleggen. Omgekeerd gelden aanvullende vereisten.

Het uitgangspunt is dat ondernemingen:

- de vakbekwaamheid van hun medewerkers borgen door hen een passende opleiding te laten doen. Dit kan een door DSI geaccrediteerde opleiding zijn of een andere opleiding die voldoet aan de vakbekwaamheidsvereisten; en
- jaarlijks de vakbekwaamheid en opleidingswensen van medewerkers evalueren.

2.2 Vakbekwaamheid niet altijd geborgd

Uit de resultaten blijkt dat de meeste respondenten de vakbekwaamheid van medewerkers hebben geborgd via een DSI-geaccrediteerde-opleiding of een andere interne of externe opleiding.

Er zijn echter ook ondernemingen die hebben aangegeven dat de vakbekwaamheid van (een deel) van hun medewerkers niet is geborgd of dat deze niet jaarlijks wordt geëvalueerd.

Ook is er een aantal ondernemingen dat de regels niet goed lijkt te kennen. Een (universitaire) opleiding al dan niet in combinatie met jarenlange ervaring is bijvoorbeeld niet voldoende om aan het criterium vakbekwaam uit de Wft te voldoen.

2.3 Ga na of u voldoet

Wij vragen u om te controleren of uw onderneming zich houdt aan de vakbekwaamheidsvereisten zoals beschreven in de Regeling vakbekwaamheid en waar nodig verbeteringen door te voeren in de inrichting en toepassing van de vakbekwaamheidsvereisten binnen uw onderneming. Dit begint met vaststellen en vastleggen welke medewerkers precies aantoonbaar vakbekwaam moeten zijn volgens deze eisen.

3. Interne controle functie

Een effectieve inrichting van interne controlefuncties is een belangrijk onderdeel van een beheerste en integere bedrijfsvoering binnen beleggingsondernemingen. Binnen het SREP vormt dit een essentieel aandachtspunt. De uitkomsten maken inzichtelijk in hoeverre ondernemingen beschikken over een effectief functionerende compliancefunctie en interne auditfunctie met passende bevoegdheden en de benodigde deskundigheid.

3.1 Opzet en bestaan compliance grosso modo in orde

Van alle ondernemingen geldt voor 9 op de 10 dat zij:

- minimaal jaarlijks het compliancebeleid herzien in samenwerking met het bestuur, en dit vastleggen;
- medewerkers (structureel) laten opleiden met betrekking tot compliance en de compliancefunctie voldoende toegang heeft tot opleidingsmogelijkheden. Ook de ervaring en senioriteit van compliancefunctie lijkt over de breedte goed met gemiddeld 10+ jaar ervaring;
- over een formeel proces beschikken voor het melden, registeren en behandelen van compliance-overtredingen.

Alle ondernemingen geven aan dat compliance directe en onbeperkte toegang heeft tot het bestuur/de directie, al blijkt dat niet overal jaarlijks een formele compliancerapportage wordt opgesteld en besproken met het bestuur. Dit laatste geldt voor ongeveer 10% van de ondernemingen.

Van de ondernemingen geeft 66% aan een compliance-monitoringsprogramma beschikbaar te hebben dat ieder jaar wordt geüpdatet en goedgekeurd.

3.2 Werking en volwassenheid baart zorgen

Alhoewel de meeste ondernemingen beschikken over een volledig of gedeeltelijk compliance monitoringsprogramma ontbreekt formele vastlegging en goedkeuring in veel gevallen. Een op de drie ondernemingen heeft geen (volledig) compliance-monitoringsprogramma. Dat betekent concreet dat er sprake is van een beperkte, ad-hoc monitoring zonder systematische aanpak. Daarnaast komt het helaas voor dat de compliancefunctie onder druk staat door tekort of gebrek aan middelen. Wat ook opvalt is dat veel ondernemingen weliswaar over een formeel compliance risicobeoordelingsproces beschikken maar dat dit niet regelmatig wordt herzien. Een andere opvallende observatie is dat er ondernemingen zijn waarvan compliance pas achteraf geconsulteerd wordt bij beleidsontwikkelingen.

4. Duurzaamheid: beleid en procedures

Een van de aandachtsgebieden die in SREP aan bod komt is het ESG-raamwerk en diens impact op de levensvatbaarheid en duurzaamheid van het bedrijfsmodel en de lange-termijn bestendigheid van de onderneming. Op het gebied van duurzaamheid hoeft het wiel niet opnieuw uitgevonden te worden. De Sustainable Finance Disclosure Regulation (SFDR) en daarop gebaseerde aanpassingen aan MiFID II bieden genoeg aanknopingspunten om een goed beeld te krijgen van ESG-risico's en verplichtingen onder beleggingsondernemingen. De vragen uit dit SREP-blok worden ook gebruikt om een goed beeld van de markt te krijgen met betrekking tot de vastlegging van ESG-gerelateerde indicatoren in beleid en procedures.

4.1 Duurzaamheidsuitingen bij meerderheid in orde

Driekwart van de beleggingsondernemingen heeft beleid om de consistentie van verplichte en onverplichte uitingen te waarborgen. Van deze 142 partijen beleggen 105 dit beleid op bestuursniveau, al lijkt expliciete vastlegging van deze betrokkenheid voor met name kleine ondernemingen te ontbreken. 78% van ondernemingen met beleid omtrent uitingen, evalueert deze minimaal een keer per jaar. Het merendeel wijst een afdeling (of gremium) aan voor goedkeuring van duurzaamheidsuitingen, een deel acht zichzelf als onderneming te klein om dit ingericht te hebben. Dat laat onverlet dat ook in die gevallen duidelijk moet zijn wie verantwoordelijk is voor de waarborging van de consistentie van uitingen.

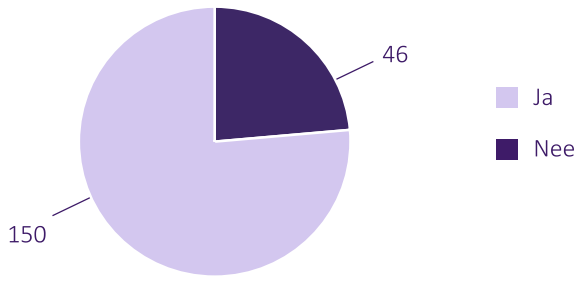
Zeker 85% heeft beleid vertaald naar concrete processen. Tweederde van de ondernemingen heeft procedures om begrijpelijkheid van uitingen aan te laten sluiten bij het klantenbestand.

4.2 Aandachtspunten

Greenwashing

Een groot deel (48%) van de ondernemingen heeft geen beleid om 'greenwashing' te voorkomen. Een nog groter deel (76%) geeft aan geen definitie van 'greenwashing' in haar beleid vastgelegd te hebben. Dit betekent ook dat 24% van de ondernemingen wél een definitie van 'greenwashing' heeft, terwijl 52% aangeeft beleid te hebben om 'greenwashing' te voorkomen. Hoe wordt dit in beleid vastgelegd, zonder het begrip te definiëren?

Figuur 4.1 Antwoordverdeling begrip greenwashing



Bevat uw beleid een definitie van het begrip Greenwashing?

Integratie van duurzaamheidsrisico's

Met betrekking tot de interne besluitvormingsprocessen, die betrekking hebben op het samenstelllen van beleggingsportefeuilles en/of het adviseren over beleggingsportefeuilles kan het volgende worden opgemerkt. Alhoewel een krappe meerderheid (61%) van ondernemingen zowel duurzaamheidsrisico's als duurzaamheidskenmerken overweegt in deze besluitvorming, geven 47 ondernemingen aan dat de verantwoording voor integratie van duurzaamheidsrisico's niet expliciet is belegd bij een of meer personen of gremia.

Vastlegging incorrecte weergave duurzaamheid

Mitigerende maatregelen met betrekking tot incorrecte weergave omtrent duurzaamheid worden veelal niet vastgelegd. Deze conclusie is in lijn met eerdere constateringen: wie immers geen definitie van 'greenwashing' in het beleid heeft vastgelegd, kan een incorrecte weergave niet constateren, laat staan hierop acteren.

5. Best execution

Best execution vormt een kernonderdeel van het gedragstoezicht op beleggingsondernemingen, want het raakt rechtstreeks aan de bescherming van cliënten, is een toetsingspunt in de bredere beoordeling van de risicobeheersing van een beleggingsonderneming en is nadrukkelijk in SREP verankerd.
Best execution is essentieel voor zowel een zorgvuldige dienstverlening als voor het beperken van risico's voor cliënten. De verplichting tot best execution raakt niet alleen de technische uitvoering van orders, maar ook aspecten zoals monitoring, rapportage en beleid.

5.1 Periodieke en systematische review

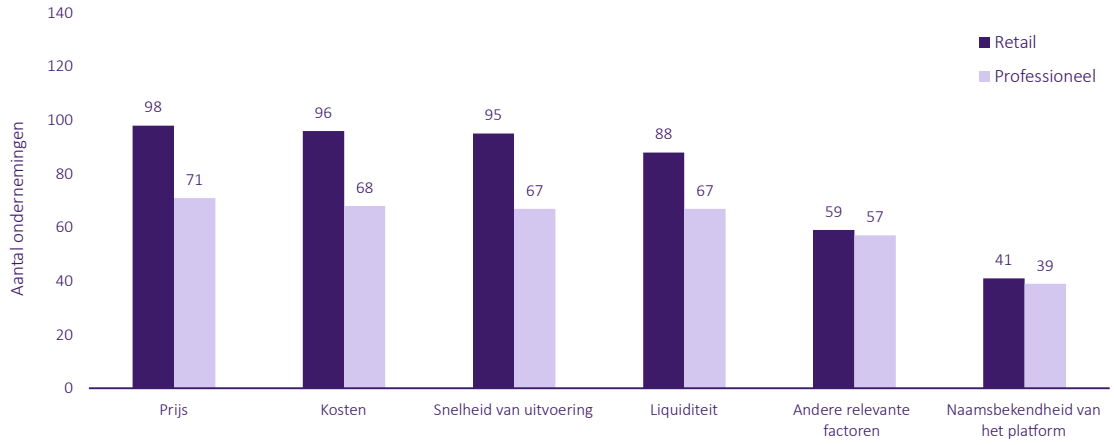
De bepalingen rondom best execution zijn van toepassing op het uitvoeren van orders van klanten en op het ontvangen en doorgeven van orders. Het merendeel van de betrokken ondernemingen (70%) heeft het orderuitvoeringsbeleid in het afgelopen jaar formeel herzien. Deze ondernemingen geven aan dat zij het beleid voor de keuze van uitvoeringslocaties en -platformen ten minste jaarlijks, en waar nodig proactief, evalueren. Daarnaast betrekt een meerderheid van de ondernemingen (60%) de tweede en derde lijn bij de monitoring en evaluatie van best execution. De overgrote meerderheid beschikt bovendien over duidelijke procedures voor het verstrekken van ordergegevens aan cliënten op een redelijk verzoek.

5.2 Structurele borging schiet te kort

Een kwart van de partijen die de kwaliteit van de structurele borging van de orderuitvoering voor hun klanten moet borgen doet dit helemaal niet of ad hoc. Daarnaast zijn er ondernemingen die aangeven orders standaard als specifieke cliëntinstructies te behandelen waardoor het resultaat voor klanten mogelijkerwijs niet conform de best execution normen is. Partijen ontlopen daarmee mogelijk de best execution verplichting.

Daarnaast is voor de helft van de bredere populatie het advies om het orderuitvoeringsbeleid gedetailleerd vast te leggen. Denk daarbij onder andere aan een duidelijk proces of regels bij beperkte liquiditeit. Bij deze vastlegging dienen meerdere uitvoeringscriteria, als liquiditeit, prijs, kosten, snelheid en operationele continuïteit van het platform in ogenschouw te worden genomen.

Figuur 5.1. Criteria voor beoordeling behalen beste resultaat – onderscheid Retail en Professioneel



Welke criteria worden gebruikt om te beoordelen of het beste resultaat voor cliënten wordt behaald?

6. Klantbediening en derden

In toenemende mate faciliteren vergunninghoudende beleggingsondernemingen derden bij het aanbieden en/of uitvoeren van vergunningplichtige activiteiten al dan niet onder een eigen handelsnaam. Daarom zijn in de SREP-uitvraag van september 2025 aan beleggingsondernemingen gerichte vragen hierover gesteld. Deze uitvraag heeft tot doel om meer inzicht te verkrijgen van de wijze waarop klantbediening plaatsvindt met inzet van derden.

6.1 Klantbediening door derden in beeld

Een op de vijf vergunninghoudende beleggingsondernemingen zet derden in bij de dienstverlening aan klanten. Driekwart van de partijen die werken met derden kent meer dan één samenwerkingsverband. Dit kan gaan om verbonden agenten, nationaal regime of andere vormen van samenwerking, waaronder zzp-ers. Op basis van de response kan worden berekend, dat het minimaal om 150 partijen of personen gaat.

Beleggingsondernemingen die werken met verbonden agenten geven aan dat deze verbonden agenten een breed scala aan diensten verlenen. In vrijwel alle gevallen gaat het hier om de combinatie het aanbrengen van cliënten, het adviseren van cliënten en het ontvangen en doorgeven van orders.
Het werken met derden kan een substantiële impact op het verdienmodel van de beleggingsonderneming hebben en raakt daarmee de duurzaamheid van het bedrijfsmodel. Zo geeft 20% van de partijen die werken met intermediaire partijen aan voor meer dan 50% van het vermogen onder beheer afhankelijk te zijn van deze derden partijen. Vergelijkbare percentages zien we terug in inkomsten en kosten.

6.2 Inzet van derden stelt hoge eisen aan de inrichting van de bedrijfsvoering

Vergunninghoudende beleggingsondernemingen die derden inschakelen en/of faciliteren om klantgerichte activiteiten uit te voeren moeten hun bedrijfsvoering dusdanig inrichten en beheersen dat er geen enkel misverstand kan ontstaan over de borging van het klantbelang en de wijze waarop verantwoordelijkheden en bevoegdheden passen binnen de door de AFM afgegeven vergunning.
De zorg is meerledig: past het servicemodel binnen de reikwijdte van de vergunning? Is het voor de eindklant duidelijk hoe de keten georganiseerd is en hoe de aansprakelijkheid is geregeld? Voldoet de kwaliteit van de bedrijfsvoering? Hoe wordt de dienstverlening aan de eindklant geborgd? Hoe wordt omgegaan met mogelijke belangenconflicten?

Met name daar waar de beleggingsonderneming zaken als directie, compliance, in- en externe rapportage(tools) faciliteert, is het niet altijd duidelijk is of er sprake is van het door derden verlenen van beleggingsdiensten in beleggingsproducten. Ook zijn de samenwerkende personen niet altijd geregistreerd bij DSI en/of hanteren zij in hun handelsnaam de term vermogensbeheer terwijl daar geen sprake van is/zou moeten zijn. In sommige gevallen bieden beleggingsondernemingen deze derden ruimte voor het (op onderdelen) zelfstandig inrichten van het beleggingsbeleid. De AFM gaat kijken of dit passend is binnen de regelgeving en zo ja verder verduidelijken welke extra eisen dit stelt aan de inrichting en monitoring van de beheerste en integere bedrijfsvoering.

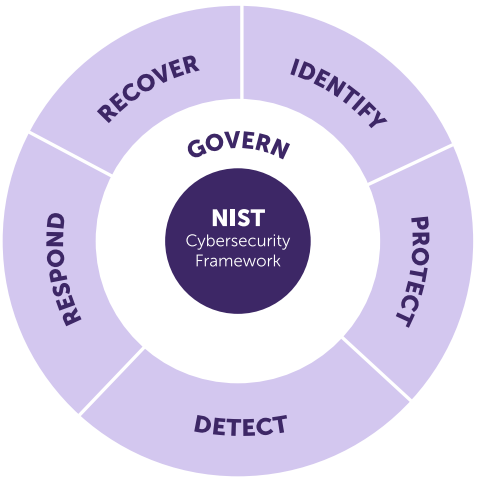
Het monitoren van de inzet van derden vraagt dus de nodige aandacht. In vrijwel alle gevallen wordt hier aandacht aan geschonken en worden elementen als werkwijze, conflict of interest en opvolging van wet- en regelgeving meegenomen en zijn meerdere vertegenwoordigers betrokken. Het is niet in alle gevallen

duidelijk of de monitoring ook adequaat wordt opgevolgd en/of de tijdsbesteding, diepgang en reikwijdte voldoende is om alle onderdelen van de samenwerking te beoordelen en aandachtspunten op te volgen.

7. ICT-risicobeheersing

ICT-risicobeheersing is bij ondernemingen nog steeds van sterk groeiend belang. Digitale processen vormen het moderne fundament van de bedrijfsvoering van financiële instellingen, hierdoor is de afhankelijkheid van ICT-systemen zeer groot. Deze digitalisering brengt efficiëntie, snelheid en schaalbaarheid, maar ook een inherente kwetsbaarheid met zich mee als ICT niet goed beheerst wordt. Voor de analyse gebruikt de AFM het NIST (National Institute of Standards and Technology) Cybersecurity Framework 2.0. De fases uit het NIST-raamwerk zijn ook verwerkt in DORA in de sectie ICT-risicobeheer. Het framework biedt een systematische aanpak om cybersecurityrisico's op een gestructureerde manier weer te geven.

Figuur 7.1. NIST Cybersecurity Framework 2.0

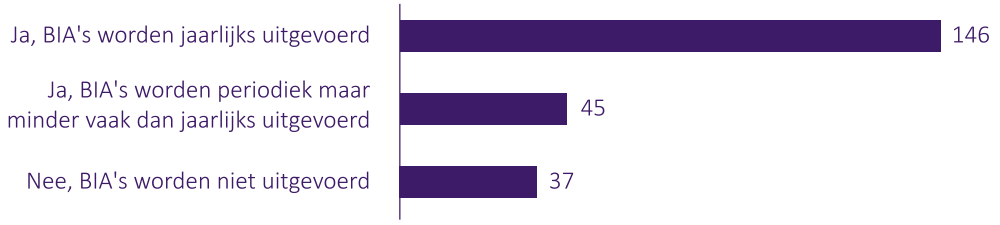


7.1 NIST Cybersecurity Raamwerk als basis

Het NIST Cybersecurity Raamwerk bevat zes samenhangende fases. De buitenste cirkel start bij het identificeren van ICT-componenten en processen. Vervolgens worden op de geïdentificeerde ICT-componenten beschermings-, alarmerings-, opvolgings- en herstelmaatregelen getroffen. Een bestuurlijke laag zorg dat de vijf technische fases worden begeleid. Deze fases zijn gebruikt in de SREP-vragenlijst. We lopen de afzonderlijke fases langs en benoemen de in het oog springende observaties.

Identify: ICT-systemen, software, processen en bedrijfsfuncties moeten geïdentificeerd en up-to-date worden gehouden. Uit de uitkomsten blijkt dat in meer dan de helft van de gevallen de ICT-werkplekken, netwerken, servers en mogelijke klantportalen zijn uitbesteed aan een ICT-dienstverlener. Hiermee ligt de rest van de technische cyclus (zoals protectie) veelal bij een derde partij. De verantwoordelijkheid voor deze cyclus ligt wel bij de instelling zelf; zij zullen dus direct moeten aansturen en afspraken maken over de uitbestede ICT-assets. Zonder inhoudelijke werkafspraken kan een instelling onvoldoende de NIST-cyclus doorlopen. Ook ziet de AFM het als een risico dat zo'n 35% van de instellingen niet of niet jaarlijks een Bedrijfsimpactanalyse (BIA) uitvoert. Hierdoor heeft een deel van de instellingen de ICT-risico's mogelijk onvoldoende in kaart.

Figuur 7.2. Frequentie waarmee Business Impact Analyses (BIA) worden uitgevoerd



Worden er Business Impact Analyses uitgevoerd (BIA) uitgevoerd binnen uw onderneming om onder andere de impact van ernstige verstoringen te identificeren?

Protect: Op ICT-assets worden preventieve maatregelen toegepast, zoals bijvoorbeeld tijdig patches installeren om kwetsbaarheden te adresseren en sterke authenticatie (twee- of andere multifactor) toepassen. Door de uitkomsten van de uitvraag heeft AFM over deze fase de meeste zorgen. Opvallend is dat uit de uitkomsten blijkt dat de regelmaat van de kwetsbaarhedenscans in de sector verschilt. Minder dan de helft van de partijen scant minimaal wekelijks op kwetsbaarheden in het ICT-landschap. Ook geeft een aantal instellingen aan helemaal geen kwetsbaarhedenscans uit te voeren. De resultaten van deze scans geven cruciale informatie voor het prioriteren van welke software kwetsbaarheden als eerste geüpdatet moeten worden, bijvoorbeeld op basis van een kwetsbaarheidsscore. Wat het risico zou beperken in dit geval, is als er concrete afspraken over de opvolging van de scans worden gemaakt met derden en externe dienstverleners.

Detect: Nadat er beveiligingsmaatregelen op ICT-assets zijn geplaatst, dienen er detectiemaatregelen op de ICT-assets worden geplaatst. In deze fase worden afwijkingen op systemen gedetecteerd. Uit de uitkomsten blijkt dat detectie het best scoort van de zes fases. 75% van de instellingen gebruikt een geautomatiseerd systeem om afwijkende ICT-activiteiten te detecteren over verschillende systemen. Dit is relatief veel. Belangrijk om te vermelden is dat meer dan de helft van de organisaties het detecteren uitbesteedt aan een derde partij. Wederom is het belangrijk dat er heldere afspraken worden gemaakt. Als er inadequaat wordt gedetecteerd heeft dit gevolgen voor de responstijd op het ICT-incident (zie volgende fase).

Respond: Als er een ICT-incident plaatsvindt, dan moeten er plannen en processen zijn om snel te reageren om de impact te verkleinen. Hierbij moet de BIA worden meegenomen. Ook worden bij zo'n 40% van de instellingen niet tenminste jaarlijks business continuity management (BCM) oefeningen gehouden. Hierdoor beheerst een deel van de instellingen hun ICT-risico's op dit vlak onvoldoende, waardoor een effectieve incidentafhandeling in gevaar komt.

Recover: Maatregelen dienen genomen te worden om herstel van systemen en data mogelijk te maken. Het valt in de SREP-uitvraag op dat bijna alle instellingen dagelijkse back-ups maken, echter het terugzetten van de back-up's wordt infrequent getest. Ongeveer 20% van de instellingen doet dit minimaal 1x per maand. De overige 80% test de back-ups jaarlijks, langer dan een jaar of zelfs helemaal niet. Het frequent testen van de bruikbaarheid van back-up's is cruciaal om herstel zoveel mogelijk te garanderen. Het te laat concluderen dat een back-up niet werkt of incompleet is, kan rampzalige gevolgen hebben.

Govern: In de doorlopende bestuurlijke fase dienen er duidelijke verantwoordelijkheden, beleid, processen en toezicht op de eerdere fases te zijn. Vrijwel alle instellingen, ruim 90%, hebben in hun risicobeheersingsraamwerk een specifiek onderdeel geïmplementeerd dat ICT-risico's adresseert. De verantwoordelijkheid voor deze operationele ICT-risico's en ICT-risico's bij derden worden bij bijna 60% van ondernemingen bij een bestuurder geplaatst en niet bij een separate rol[1]. Dit kan proportioneel zijn, maar dan is het essentieel dat een bestuurder adequate ICT-kennis heeft om deze risico's te beheersen.

7.2 Volwassenheid van fases baart zorgen

Instellingen hebben over het algemeen maatregelen genomen om hun organisatie te beschermen tegen ICT-risico's. Op niet alle vlakken lijkt dat echter voldoende ingevuld. De instellingen geven aan het meeste aan de detectie fase te voldoen. De AFM is het meest bezorgd over de protectie fase. De toename van het aantal cyberaanvallen geeft aanleiding goed te onderzoeken of bepaalde basis cyberhygiëne maatregelen voldoende zijn ingericht en geëffectueerd. Dit kan intern of extern zijn bij een derde partij. Een belangrijke maatregel is bijvoorbeeld het tijdig en frequent patchen en het toepassen van sterke toegangscontrole (zoals multifactor authenticatie).

[1] DORA vereist in beginsel dat de verantwoordelijkheid voor ICT-risico in een separate functie wordt geplaatst.