ANALYSE SECTOR IN BEELD

SREP Marktbeeld: terugkoppeling van de belangrijkste bevindingen

In het kort Met ingang van 1 januari 2023 zijn de Supervisory Review and Evaluation Proces-richtsnoeren (SREP) voor beleggingsondernemingen ingevoerd. In 2023 zijn door de AFM twee SREP-vragenlijsten verstuurd naar 240 beleggingsondernemingen. Het betreft zowel vermogensbeheerders als beheerders van beleggingsinstellingen met een MiFID-top up als Handelaren voor Eigen Rekening (HER's) en handelsplatformen. In dit SREP Marktbeeld geven we een marktbrede terugkoppeling van de resultaten op het gebied van integere en beheerste bedrijfsvoering.

Inleiding

Aan de hand van deze terugkoppling kunt u nagaan of u nog verbeteringen kunt aanbrengen in uw bedrijfsvoering. Daarbij is de nadruk gelegd op een aantal in het oog springende observaties op het gebied van ICT-beheersing, Product Approval & Review Proces (PARP), governance, vermogensscheiding en management.

Eerste observaties

ICT-beheersing

Een goede beheersing van de ICT is, naast het waarborgen van de bedrijfsprocessen van de instelling, om drie redenen belangrijk:

1. Het verkleint het risico op misstanden in de keten (in het geval van uitbesteding);
2. Cyberrisico's in de vermogensbeheermarkt nemen toe. Dit kan leiden tot verstoringen in de dienstverlening aan (eind)klanten;
3. Er komt nieuwe wet- en regelgeving voor de sector aan (DORA). Een goede ICT-beheersing is de basis van DORA compliance.

In de eerste SREP-uitvraag is aan beleggingsondernemingen gevraagd een inschatting te maken van de volwassenheid van het ICT-risicobeheersingsniveau. Hiervoor is gebruik gemaakt van een selectie aan beheersmaatregelen uit de DNB Good Practice Informatiebeveiliging. Opvallend genoeg bleken veel beleggingsondernemingen relatief onbekend met de DNB Good Practice Informatiebeveiliging en/of gingen zij voor het eerst aan de slag met deze manier van uitvragen (een self-assessment).

De tweede uitvraag bestond uit meer gesloten vragen. Hieruit bleek dat een derde van de beleggingsondernemingen nog een verbeterslag kan maken als het gaat om het opzetten en/of beheren en/of vaststellen van hun *ICT-risk management framework*. Opvallend, want juist een vastgesteld *ICT-risk management framework* is het startpunt van goed ICT-risicobeheer. In het *ICT-risk management framework* geeft de instelling namelijk aan hoe het omgaat met risico's op het gebied van informatiebeveiliging.

Verder blijkt uit de resultaten dat één op de drie beleggingsondernemingen niet regelmatig risicoanalyses uitvoert. Beleggingsondernemingen lopen hierdoor het risico dat zij niet op de hoogte zijn van alle huidige en potentiële (cyber)dreigingen waar zij mee te maken hebben.

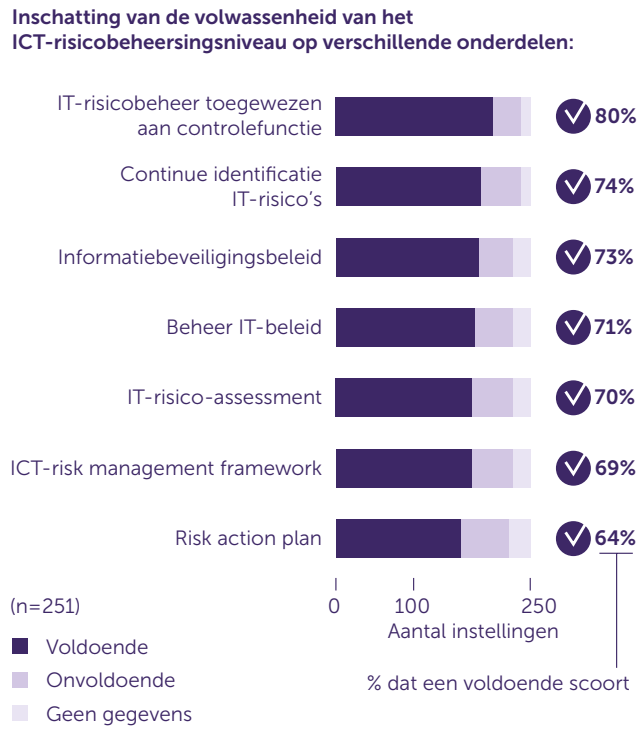
Tenslotte viel op dat veel beleggingsondernemingen geen *Business Impact Analyse* (BIA) uitvoeren en/of beschikken over een *risk action plan*. Een BIA en een *risk action plan* zijn overigens twee verschillende zaken: na een risico-analyse maak je een plan om een risico te verkleinen, dat is het *risk action plan*, een BIA maak je als startpunt van je

JULI 2024

AFM

Business Continuity Plan (BCP). In een *risk action plan* staat hoe ondernemingen omgaan met de risico's die niet voldoende worden verkleind door de bestaande beveiligingsmaatregelen. Bij het ontbreken van een *risk action plan* kunnen risico's grote schade aanrichten aan de betreffende beleggingsonderneming en/of het financiële systeem.

Figuur 1. ICT-risicomanagement



Wat zien we in figuur 1?
Hoeveel procent van de ondernemingen beoordeelt haar ICT-risicomanagement als voldoende? In deze tabel is de score uitgesplitst naar een aantal elementen die onderdeel uitmaken van het ICT-risicomanagementframework.

Wel geven de meeste beleggingsondernemingen aan dat zij een onafhankelijke controlefunctie hebben ingericht die verantwoordelijk is voor het beheer en toezicht op ICT-risico's.

De SREP-uitkomsten geven ook een beeld van de onderwerpen van ICT-beheersing die beleggingsondernemingen lastig lijken te vinden. Het gaat dan specifiek om het testen van hun digitale operationele weerbaarheid en het testen van het *Business Continuity Plan*. Door regelmatig te testen krijgt een onderneming inzicht in de feitelijke weerbaarheid van hun processen en systemen.

Veel beleggingsondernemingen geven zichzelf een onvoldoende op het gebied van crisiscommunicatieplannen. Hierbij is als richtlijn aangehouden dat ondernemingen moeite hebben met een onderwerp wanneer minder dan 75% van de ondernemingen voldoende scoort.

Product Approval & Review Proces

Een goed ingericht Product Approval & Review Proces (PARP) is belangrijk, omdat:

1. Het de product- en distributiestrategie expliceert;
2. Het inzicht geeft in de evenwichtige belangenafwegingen die moeten worden gemaakt bij het in de markt zetten van nieuwe producten en/of diensten;
3. Het de basis vormt voor de uitwerking van de (keten)processen.

Op het gebied van PARP is nog werk aan de winkel. Te veel beleggingsondernemingen (ruim 20%) denken namelijk onterecht dat PARP niet op hen van toepassing is.

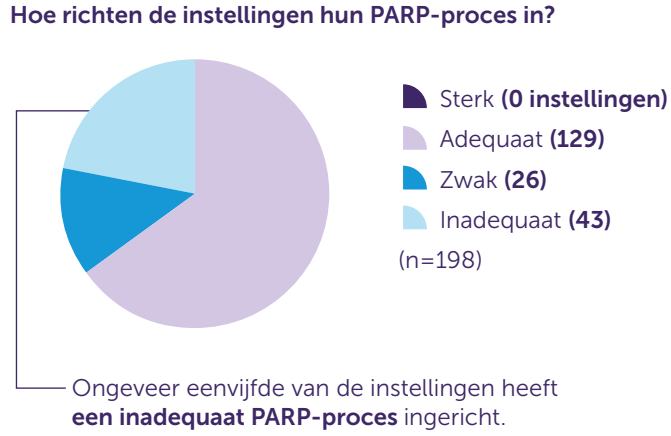
Sommige beleggingsondernemingen zijn van mening dat PARP niet op hen van toepassing is, omdat ze alleen vermogensbeheer aanbieden of beleggingsdiensten leveren. Andere beleggingsondernemingen denken niets met PARP te hoeven doen omdat ze geen eigen producten maken, alleen met professionele relaties werken of uitsluitend externe beleggingsoplossingen selecteren. Ook in bovenstaande omstandigheden geldt dat beleggingsondernemingen PARP moeten hebben.

Het Product Approval & Review Proces wint aan kwaliteit als:

a. Vanuit meerdere invalshoeken naar een vraagstuk wordt gekeken. Bijvoorbeeld: niet alleen vanuit Juridische Zaken en/of Compliance, maar ook vanuit risicomanagement, operations en productmanagement.
b. Meerdere aspecten worden meegenomen in de beoordeling, zoals afgebakende doelgroep, distributiestrategie en wijze van informatieverstrekking. Ook een duidelijke scheiding van verantwoordelijkheden, het toetsen van scenario's en niet te vergeten een periodieke evaluatie van producten en diensten horen bij het proces.
c. De doelgroepsbepaling gestructureerd wordt uitgevoerd. Daarbij gaat het dan om elementen als risicotolerantie, duurzaamheid, beleggingshorizon, klantlocatie, -kennis en ervaring en de kosten.

Alhoewel het Product Approval & Review Proces niet op alle partijen (zoals HER's) van toepassing is, blijkt uit onderstaande figuur dat een derde van de beleggingsondernemingen waarvoor wel de verplichting geldt geen PARP-proces heeft ingericht en/of dat de inrichting nog te wensen overlaat.

Figuur 2. SREP-scores PARP



Wat zien we in figuur 2?
De grafische weergave van de SREP-scores op PARP. Op basis van de analyse van de uitkomsten van deze eerste SREP-PARP mag worden opgemaakt dat 2/3 van beleggingsondernemingen het PARP adequaat heeft ingericht. Een op de drie beleggingsondernemingen waarvan verwacht mag worden dat ze een PARP hebben ingericht scoren onvoldoende ('zwak') of hebben zelfs nog geen PARP ingericht ('inadequaat').

Governance: beleid en interne beheersing

In de eerste SREP-uitvraag is een inventarisatie gemaakt rond het thema interne risicobeheersing. Het gaat onder andere om beleidsstukken, (risico)frameworks, gedragscodes en procedures.
Een goede governance is belangrijk omdat het inzicht geeft in de wijze waarop de onderneming:

1. Is ingericht met oog op het borgen van de benodigde functiescheiding;
2. De effectiviteit van beheersmaatregelen borgt;
3. Zorgt voor een adequate en actuele vertaling van wet- en regelgeving naar procedures en processen.

Een zeer ruime meerderheid (>90%) geeft aan op het thema 'interne beheersing' over beleid te beschikken. Al betekent dit niet meteen dat ze dit beleid ook goed hebben vastgelegd en dat dit beleid goed wordt geïmplementeerd. Een aanzienlijk deel van de beleggingsondernemingen (20%) moet nog beleid opstellen (en implementeren) rondom andere thema's, zoals het aangaan van leningen en/of andere transacties met bestuurders, en het implementeren van de klokkenluidersregeling.

Vermogensscheiding

Een goede vermogensscheiding is belangrijk, omdat het bijdraagt aan:

1. De verbetering van de beleggersbescherming;
2. De financiële stabiliteit van de sector;
3. De beheerste bedrijfsvoering door heldere administratieve inrichting en controle.

Uit de resultaten blijkt dat beleggingsondernemingen weinig inzicht lijken te hebben in de dienstverlening van (de door hen aangestelde) depotbanken. Klanten van deze beleggingsondernemingen zijn juist gebaat bij dit inzicht.

Met name in het institutionele segment geven beleggingsondernemingen aan niet altijd op de hoogte te zijn van de afspraken die gemaakt zijn tussen de institutionele belegger en haar depotbank. Met name als het gaat over het onderwerp *securities lending*. Als een beleggingsonderneming onvoldoende op de hoogte is van de manier waarop institutionele beleggers hun bewaarfunctie hebben ingericht, kan dit impact hebben op hun bedrijfsvoering.

Een beleggingsonderneming moet ook informatie kunnen verstrekken aan cliënten over wat er met hun stukken gebeurt in het kader van *securities lending*. Mocht de beleggingsonderneming meerdere depotbanken gebruiken - waarvan de één wel stukken uitleent en de ander niet - moeten cliënten dit weten. Daarnaast is het ook relevant of de klant ook de volledige opbrengst van het uitlenen ontvangt.

Management

Bij de uitvragen over de inrichting van het management is gekeken naar samenstelling en betrokkenheid van het bestuur, de functiescheiding en de (doorlopende) geschiktheid van bestuurders. Het meten van deze aspecten is belangrijk, omdat een gezonde samenstelling, beschikbaarheid en betrokkenheid een randvoorwaarde is voor:

1. De continuïteit van de beleggingsonderneming;
2. Het borgen van de benodigde functiescheiding;
3. De doorlopende toets op geschiktheid.

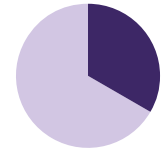
Een derde van de beleggingsondernemingen geeft aan dat er bij hen sprake is van een ‘compacte organisatie’; een organisatie waarbij de directie zelf alle rapportages maakt en/of dusdanig betrokken is bij de dagelijkse bedrijfsvoering, dat zij op die manier dus altijd op de hoogte is van de gang van zaken. Maar ‘op de hoogte zijn’ is niet voldoende. Betrokkenheid van bestuur, en de functiescheiding, moet formeel worden vastgelegd.

180 respondenten gaven in open vragen inzicht in de mate waarin het bestuur van hun onderneming op de hoogte is van de activiteiten, de financiële situaties en de daaraan gerelateerde risico’s. Een derde tot de helft van deze beleggingsondernemingen is in ieder geval regelmatig op de hoogte van de ontwikkelingen.

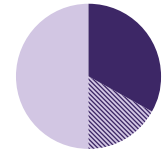
In een markt die volop in beweging is, hetgeen zich onder andere uit in overnames, fusies, samenwerkingsverbanden en/of wijzigingen in het bedrijfsmodel (inclusief uitbesteding), valt het de AFM op dat 40% van de partijen aangeeft nooit of niet recent (in de afgelopen zes jaar) contact te hebben gehad met de toezichthouder over significante wijzigingen in de organisatie en/of wijzigingen in geschiktheid bestuurders, terwijl het wel verplicht is om dit soort zaken te melden aan de AFM.

Figuur 3. Open antwoorden op een aantal managementvragen

Inrichting van het management



Eenderde van de respondenten (n=251) vindt dat er sprake is van een ‘compacte organisatie’.



Eenderde tot de helft van de respondenten (n=180) vindt dat het bestuur van hun onderneming regelmatig op de hoogte is van ontwikkelingen van activiteiten, financiële situaties en de daaraan gerelateerde risico’s.

40% van de respondenten (n=251) geeft aan in de afgelopen zes jaar nooit contact gehad met de toezichthouder over significante wijzigingen in de organisatie en/of wijzigingen in geschiktheid bestuurders.

Wat zien we in figuur 3?
In deze figuur is de analyse van de open antwoorden op een aantal vragen rondom het thema management zoals deze eerder is beschreven grafisch weergegeven.

Werkwijze en scores

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 zo-genoemde SREP-scores. SREP werkt met een doorlopende normering van 1 tot 4, waarbij een 1 staat voor 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.

Nieuwe uitvraag in september

In september 2024 komt onze volgende SREP-uitvraag. U wordt daar nog uitgebreid over geïnformeerd. Naast een aantal terugkerende datavelden die bijdragen aan het beeld van de bedrijfsvoering, zullen we dit jaar onder andere stil staan bij klachten en incidenten, uitbesteding en beloningsbeleid. Een paar weken voordat de vragenlijst ter beantwoording open wordt gezet in het AFM Portaal ontvangt u de aankondigingsbrief en ter voorbereiding een pdf van de vragenlijst.