Software Improvement Group

Datum Amsterdam, 30 augustus 2016
Onderwerp Reactie SIG op Discussiedocument AFM-DNB

Geachte dames en heren,

Naar aanleiding van het gepubliceerde discussiedocument *Meer ruimte voor innovatie in de financiële sector*, d.d. 9 juni 2016, willen wij graag onze reactie en onze feedback hierop met u delen.

Wij zien dat de toezichthouders zich vooral richten op het waarborgen van een robuuste financiële dienstverlening. De financiële sector en de innovatie daarin worden echter meer en meer gedreven door informatietechnologie. De opkomst en populariteit van FinTechs onderstrepen dat. Een robuuste financiële dienstverlening vereist volgens ons daarom vooral een robuuste IT. Het toezicht daarop zal zich om die reden meer en meer moeten richten op het toezicht op de IT-middelen waarmee deze dienstverlening wordt geleverd.

Wij zijn van mening dat dit betekent dat het toezicht op de financiële dienstverlening moet worden aangepast aan deze sterk veranderende rol van IT in de totstandkoming daarvan. Met deze brief willen wij onze ideeën presenteren ten aanzien van deze aanpassingen. Het doel van de aanpassingen moet volgens ons zijn dat meer ruimte wordt geboden aan innovatie in de financiële sector. Dit moet worden gerealiseerd door zowel het toezicht laagdrempeliger te maken door lagere kosten maar tegelijkertijd meer zekerheid te bieden over de robuustheid van de IT en daarmee de financiële dienstverlening.

Huidig toezicht

Het huidige toezicht van de DNB richt zich wat betreft de IT-component van de financiële dienstverlening vooral op de informatiebeveiliging, vormgegeven in het toetsingskader gebaseerd op COBIT en geoperationaliseerd in het Self-Assessment Framework voor Informatiebeveiliging.
Deze benadering heeft echter naar ons idee drie beperkingen:

1. Dit toetsingskader is sterk gericht op documentatie;
2. Niet alle innovaties vallen vanaf het begin onder dit toezicht;
3. De toetsing vindt plaats middels een self-assessment.

1. *Documentatie biedt geen zekerheid over feitelijke situatie*

   Het Self-Assessment omvat een uitgebreide verzameling ‘control measures’, welke vooral gericht zijn op de schriftelijke vastlegging van beleid en beleidsmaatregelen en de vertaling daarvan in procesbeschrijvingen.

   Deze vorm van toezicht is kostbaar, omdat nieuwe toetreders een significante investering in tijd en geld moeten doen voor het opstellen van een auditwaardige set documentatie. Daarbij biedt het hebben van deze documentatie nog geen garantie voor een robuuste (IT) dienstverlening.

Software Improvement Group B.V.
Bezoekadres Rembrandttoren / Amstelplein 1 / Amsterdam
Postadres Postbus 94914 / 1090 GX Amsterdam
+ 31 20 314 09 50 / info@sig.eu / www.sig.eu
KvK Amsterdam 34133013

Maar bovenal wordt niet vastgesteld of het gedocumenteerde ook daadwerkelijk overeenkomt met de praktijk, laat staan of het beleid, de maatregelen en de processen effectief is en er dus een kwalitatief goede informatiebeveiliging is.

2. *Innovaties starten doorgaans buiten het huidige toezicht*
   Het Self-Assessment is van toepassing op financiële instellingen die vallen onder het toezicht van DNB en/of AFM, oftewel vergunninghouders. Een steeds groter deel van de innovatie in de financiële sector vindt echter plaats in FinTechs die niet onder dit toezicht vallen omdat zij (nog) geen vergunninghouder zijn of doordat zij hun innovatieve (IT) oplossingen aanbieden aan bestaande financiële instellingen.

   Wij onderscheiden hierbij enerzijds FinTechs die nieuwe, op IT gebaseerde, financiële diensten ontwikkelen en zelf op de markt aanbieden, en anderzijds FinTechs die nieuwe IT-oplossingen ontwikkelen en die aan bestaande vergunninghouders aanbieden.
   In beide gevallen komt de nieuwe, op IT gebaseerde innovatie pas onder het toezicht te vallen op het moment dat deze wordt ingezet voor het leveren van financiële diensten door een (nieuwe of een bestaande) vergunninghouder. Doordat het product of de dienst reeds een bepaalde leeftijd en omvang heeft bereikt, waardoor mogelijk een grote investering vereist is om aan de criteria van de toezichthouder te voldoen. In het eerste geval zal de innovatie direct onder het toezicht vallen, in het tweede geval is het toezicht indirect via de bestaande vergunninghouder. In beide gevallen kan de investering die benodigd is om op dat moment te kunnen voldoen aan het toetsingskader belemmerend werken.

3. *De betrouwbaarheid en daarmee de waarde van een Self-Assessment is beperkt*
   Het huidige toezicht op de Informatiebeveiliging is voor een groot deel gebaseerd op een self-assessment. De betreffende financiële instelling moet daarbij zelf inschatten of bepaalde documentatie en processen in voldoende mate aanwezig zijn en van voldoende kwaliteit zijn. Doordat de criteria waaraan moet worden voldaan per eis niet objectief zijn vastgelegd, is de objectiviteit en daarmee de betrouwbaarheid van de uitkomst van het self-assessment beperkt.

Samenvattend, stellen wij dat het huidige toezicht enerzijds onvoldoende waarborgen biedt voor een robuuste dienstverlening en tevens belemmerend werkt voor nieuwe innovaties doordat een grote investering in documentatie is vereist.

Ons advies voor uitbreiding en vereenvoudiging van het toezicht

Op basis van bovenstaande, lijkt het ons verstandig om bestaande wet- en regelgeving aan te passen en het toezicht op de IT-middelen van vergunninghouders te baseren op de volgende principes:

1. Toets op productkwaliteit in plaats van documentatie;
2. Toets op objectief meetbare criteria;
3. Toets periodiek met behulp van een objectieve derde.

1. *Toets op productkwaliteit in plaats van documentatie*

   Het toezicht zou naar onze mening gebaat zijn met een eenvoudige doch effectieve toets op de informatiebeveiliging en daarmee de robuustheid van de IT-oplossing. De toetsing zou zich daarom meer moeten richten op het resultaat oftewel het product, in plaats van op de documentatie. Enkel toets op de IT-producten zelf laat pas zien of beleid en processen werkelijk geïmplementeerd zijn en effectief zijn, en feitelijk hebben geleid tot een robuuste en veilige IT-oplossing.

   Dit maakt het voor nieuwe toetreders makkelijker, omdat het een enorme investering in documentatie voorkomt terwijl (de kwaliteit van) het product voor hen een kernactiviteit is. Op de langere termijn is een goede borging van beleid en processen in documentatie natuurlijk ook van belang, maar dit kan ook in een latere levensfase van de nieuwe toetreder aangezien het resultaat (het product) al onder het toezicht valt.

   Hiermee wordt de toets voor de innovatiepartij goedkoper, terwijl het ook waarde genereert voor haar genereert in de vorm van een (aantoonbaar) kwalitatief goed product.

2. *Toets op objectief meetbare criteria*

   De waarde van de toetsing of het self-assessment is groter wanneer deze is gebaseerd op meer objectieve en meetbare criteria. De Software Improvement Group heeft goede ervaringen met het toetsen van productkwaliteit aan de hand van de ISO-25010 standaard voor softwarekwaliteit. De modellen en meetinstrumenten die zij daarvoor heeft ontwikkeld, worden ingezet in diverse situaties zoals het oplossen van kwaliteitsproblemen, bij leverancierselecties, in (conflicten bij) uitbestedingsrelaties en in due diligence trajecten.

   Uitgaande van de huidige wetgeving met betrekking tot informatiebeveiliging, zou een objectieve toets zich moeten richten op het meten van de kwaliteitsaspecten onderhoudbaarheid, beveiligbaarheid en betrouwbaarheid. De criteria voor deze toets dienen te worden verankerd in de werkwijze en het softwareontwikkelproces van de vergunninghouder. Hiermee kan het toezicht reeds aanvangen in een vroegtijdig stadium van de innovatie.

3. *Toets periodiek met behulp van een objectieve derde*

   De robuustheid en beveiliging van de IT-producten van financiële instellingen is naar onze mening dusdanig belangrijk dat het toezicht daarop niet gebaseerd kan worden op enkel een self-assement. Een toets door een onafhankelijke derde biedt meer zekerheid.

   Omdat een toets op de gehele IT-omgeving van de vergunninghouder wederom duur is en daarmee belemmerend kan werken, stellen wij voor deze toets jaarlijks op een wisselend deel van de IT-omgeving uit te voeren. De scope-bepaling dient te worden gebaseerd op het risico en het belang van de IT-middelen voor de dienstverlening. De opvolging van bevindingen dient echter organisatie breed plaats te vinden, om te voorkomen dat andere IT-producten dezelfde zwakheden bevatten.

> In geval van een bestaande vergunninghouder die een innovatie adopteert, kan deze toets door een objectieve derde ook gebruikt als invulling van het indirecte toezicht.

Doordat deze toets gericht is op de kwaliteit van het IT-product, is geen additionele investering vereist om te kunnen voldoen aan alle eisen uit het toetsingskader. Het zou immers al het doel van de innovatiepartij moeten zijn om een robuust en veilig product te ontwikkelen. Hierdoor wordt het toezicht eenvoudiger en meer laagdrempelig, waardoor het toezicht eenvoudiger is uit te breiden naar financiële diensten die nog niet onderwerp van toezicht zijn door scope of omvang. Daardoor worden nieuwe innovatieve dienstverleners minder beperkt in hun toetreding en groei. Tevens biedt het de toezichthouder eerder en meer garanties dat de technologie voldoende robuust is op het moment dat de innovatie wordt ingezet voor het leveren van financiële diensten en dus onder het toezicht valt.

Onze concluderende reactie op het discussiestuk

De Software Improvement Group is van mening dat het toezicht op de financiële dienstverlening moet worden aangepast aan de sterk veranderende rol van IT in de totstandkoming van deze dienstverlening. Daarbij moeten tevens de veranderingen op het gebied van innovatie worden meegenomen en in het bijzonder het toezicht op de innovatie binnen FinTechs.

Een nieuwe manier van vergunningverlening en toezicht zou zich meer moeten richten op het daadwerkelijke IT-product en minder op documentatie van beleid en processen. Door het vaststellen van een objectief toetsingskader kunnen deze criteria reeds in een vroeg stadium van innovatie tegen lage kosten worden opgenomen en getoetst. De uiteindelijke toets dient vervolgens door een objectieve derde partij te worden gedaan op het moment van de vergunningaanvraag.

De introductie van een *beperkte vergunning* of *vergunning onder voorwaarden* lijkt ons een goed idee omdat dit naar onze mening ook de mogelijkheid biedt tot een gefaseerde opbouw van het toezicht. In deze fase zou een minder stringente toets kunnen worden gehanteerd bij toetreding, waarbij de opvolging van de gesignaleerde tekortkomingen gedurende de beperkte vergunning dienen te worden opgelost. Dit biedt nieuwe toetreders de mogelijkheid stapsgewijs zich te ontwikkelen, met een grotere kans dat men op het moment van de vergunningaanvraag eenvoudig kan voldoen aan de voorwaarden.
Een toets op het product is niet alleen minder belastend voor de (adspirant) vergunninghouder en er is ook minder additionele inspanning vereist om aan de eisen te voldoen omdat het leveren van een veilig en robuust IT-product sowieso al haar streven zou moeten zijn.
De toets biedt de toezichthouder tevens een grotere garantie dat er ook daadwerkelijk sprake is van een robuuste dienstverlening.

Door de toets reeds in een vroeg stadium van de innovatie te introduceren, zijn de kosten voor de (adspirant) vergunninghouder van zowel de toetsing maar vooral ook van de opvolging van eventuele bevindingen veel lager. Hierdoor is het mogelijk innovaties eerdere onder het toezicht te stellen, waardoor de toezichthouder reeds in een veel eerder stadium inzicht verkrijgt in de robuustheid van de innovatie.

Wij zijn van mening dat deze aanpassingen bijdragen aan een verantwoorde innovatie in de financiële sector. Graag willen wij daarom met u het gesprek aangaan over onze ideeën en voorstellen. Enerzijds om onze ideeën nader toe te lichten en om vragen van uw kant te beantwoorden. SIG biedt ook aan om betrokken te worden bij de nadere uitwerking ervan in het nieuwe toezicht, zoals een concrete

Met vriendelijk groet,

Software Improvement Group B.V.

Dr. ir. R.H. Klompé
r.klompe@sig.eu
06 – 23 12 34 66