De invloed van FinTech en de verwerking in de systematische integriteitrisico-analyse

Drs. R.M.L. Noordhoek CCP

Voorwoord

In 2015 bezocht een delegatie van Achmea ter inspiratie Silicon Valley. Een idee waarmee de verzekeraar terugkwam leidde onder andere tot kamervragen en discussie bij De Wereld Draait Door. Tegen korting op de premie voor de autoverzekering konden klanten een kastje in hun auto laten installeren om het rijgedrag te kunnen meten, om daarmee de risico's voor de verzekeraar beter in kaart te kunnen brengen. Achmea zag het waarschijnlijk als een win-win situatie, maar zo keek niet iedereen hiernaar.[1]

Beschikt men wel over een keuze om gegevens wel of niet openbaar te maken? Wat is de prijs van privacy en wat zijn de kosten? Maar ook de vraag of deze gegevens niet misbruikt zullen worden, en wat voor ontwikkelingen er op dit gebied eigenlijk nog meer zijn; zomaar een aantal vraagstukken die bij De Wereld Draait Door werden besproken.[2]

Waar het hierboven over gaat is kort samen te vatten als een reactie op de risico's van technologische ontwikkelingen in de financiële sector (FinTech). Wat FinTech nu is en welke mogelijke integriteitrisico's, ethische dilemma's en vraagstukken dit met zich meebrengt zal worden besproken in dit artikel. Ook zal worden bekeken hoe technologie juist invloed kan hebben op de beheersing van integriteitrisico's. Dit laatste wordt ook vaak omschreven als RegTech (Regulatory Technology).

1 www.google.nl/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=achmea+bezoekt+silicon+valley, laatst geraadpleegd op 12 februari 2017.
2 dewereldraaitdoor.vara.nl/media/346768, laatst geraadpleegd op 12 februari 2017.

Inleiding

Doelgroep

Dit artikel is met name geschreven voor compliance officers binnen de financiële sector, die bekend zijn met en betrokken zijn bij de compliancerisicoanalyse, ook wel systematische integriteitrisicoanalyse (SIRA)[3] genoemd.

Doel

Het is belangrijk om te weten dat FinTech een goede ontwikkeling kan zijn en het kansen oplevert om meer mensen/bedrijven op een betere manier te kunnen helpen. De 'manier waarop' technologie wordt gebruikt bepaalt of dit een goede of slechte ontwikkeling is. Het is daarom vanuit complianceperspectief essentieel om te zien hoe FinTech zich in de sector manifesteert, opdat kansen en bedreigingen ten aanzien van integriteit vroegtijdig in kaart worden gebracht.

De SIRA is daarbij een fundamenteel onderdeel voor het uitvoeren van de compliancefunctie middels de compliancecyclus, zoals beschreven in het Handboek Compliance Professional[4]. Het is een methode die gebruikt wordt voor het identificeren en beheersen van integriteitrisico's.

Dat het inzichtelijk maken van de effecten van FinTech de aandacht moet hebben van compliance blijkt ook uit de volgende passage in de toezichtvooruitblik 2017 van DNB:

> *"In de tweede helft van 2016 is een begin gemaakt met het beoordelen van de inhoudelijke kwaliteit van SIRA's en de vertaling naar de praktijk. In 2017 willen we hier een breder vervolg aan geven, waarbij diepgaand wordt onderzocht in hoeverre de SIRA daadwerkelijk leidt tot een juiste risicoafweging en een passend beheersingsbeleid. In het bijzonder richten we onze aandacht op de analyse door financiële instellingen van: (…) (2) initiatieven op het gebied van FinTech.[5]"*

Het doel van dit artikel is om te kijken naar huidige en toekomstige FinTech-ontwikkelingen en de risico's en mogelijkheden van FinTech met behulp van de SIRA-methodiek te benaderen. Deze methode kan als handvat dienen bij het implementeren van FinTech ontwikkelingen in de SIRA.

3 Dit betekent ten minste het begrijpen van de SIRA methode zoals DNB deze beschrijft in: 'DNB, De integriteit-risicoanalyse', 2015.

4 Nederlands Compliance Instituut (2016), *Handboek Compliance Professional 2016-2017*, Capelle aan den IJssel: NCI.

5 www.dnb.nl/binaries/Toezicht%20Vooruitblik%202017_tcm46-349591.pdf, laatst geraadpleegd op 23 december 2016.

Vraagstelling

De vraagstelling van dit artikel is tweeledig:

- Wat is de invloed van FinTech op integriteitrisico's in de financiële sector?
- Hoe kan dit worden verwerkt in de SIRA?

Om de eerste vraag te beantwoorden zal eerst worden ingegaan op de definitie van FinTech, RegTech en de 'krachten' die de ontwikkeling en manifestatie van FinTech mogelijk maken. Onder krachten wordt verstaan: dat wat van invloed is op de financiële sector. Hieronder vallen bijvoorbeeld technologie, wetgeving, toezichthouders.

Bij de beantwoording van vraag twee wordt met een aangepaste SIRA-methode beschreven hoe FinTech kan worden verwerkt bij het uitvoeren van de SIRA. Bij deze methode wordt onderscheid gemaakt tussen de risico's die de onderneming nu al (kan) lopen en toekomstige risico's. De laatste categorie kan ook worden gezien als de categorie integriteitrisico's die zich manifesteren bij de ontwikkeling of overname van nieuwe producten/diensten en/of organisatievormen. Zo wordt deze methode wellicht ook bruikbaar voor het PARP. Wat zal blijken is dat FinTech niet als apart thema in de SIRA moet worden opgenomen.

FinTech

De term FinTech is in praktijk erg ambigue. Dit heeft met name te maken met de definitie van technologie. De gehanteerde definitie van technologie luidt: *"een systeem dat gebaseerd is op de toepassing van kennis, dat zich manifesteert in fysieke objecten en vormen van organisatie voor het behalen van bepaalde doelen.*[6]*"*

Dit betekent dat FinTech kan leiden tot betere en nieuwe producten en diensten, maar ook tot nieuwe bedrijfsmodellen en andere toetreders in de financiële sector. Hoewel technologische ontwikkeling in de financiële sector ongeveer even oud is als de sector zelf, wordt FinTech op dit moment vooral gebruikt om gecomputeriseerde, technologische ontwikkelingen te duiden. Dit wordt vaak impliciet verondersteld wanneer men van FinTech spreekt.[7] In dit artikel wordt echter uitgegaan van de bredere definitie van technologie om FinTech aan te duiden.

RegTech

Technologische ontwikkeling kan ook zorgen voor verbeteringen in het interne en externe toezicht op financiële ondernemingen. Dit wordt RegTech genoemd, een afgeleide vorm van FinTech.

6 Volti (1992): *Society and Technological Change*, Worth Publishers.

7 Presentatie: Don Ginsel (Holland Fintech), NVB Bijeenkomst: FinTech en compliance(risico's), laatst geraadpleegd op 12 oktober 2016.

RegTech wordt hier gedefinieerd als: technologische ontwikkeling die (1) de naleving van wet- en regelgeving door, alsmede (2) het toezicht op financiële ondernemingen tracht te verbeteren.[8] Bij dit laatste wordt ook wel gesproken van Sup(ervisory)Tech.

Manifestatie van FinTech en RegTech in de financiële sector

Het kan lastig zijn om overzicht te krijgen in alle ontwikkelingen en de wijze waarop deze zich in de sector manifesteren. Het louter opsommen van de verschillende gecomputeriseerde technologieën zoals blockchain, big data en artificial intelligence is niet voldoende om een goed beeld te krijgen. De kans is groot dat daarmee niet alle ontwikkelingen in kaart worden gebracht die impact kunnen hebben op een organisatie. Door één technologie te onderzoeken kan namelijk kokervisie ontstaan.

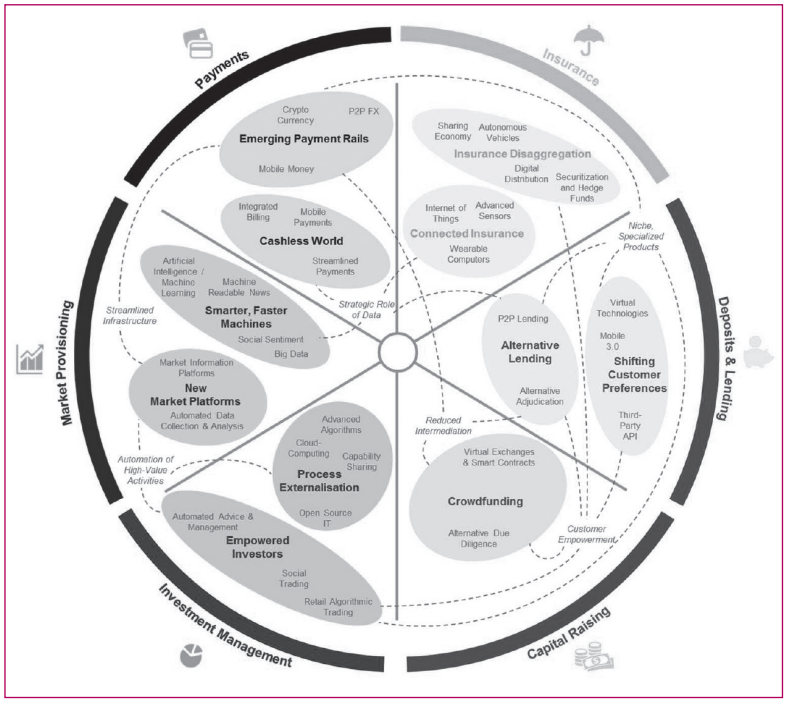
Het World Economic Forum (WEF) heeft een overzicht ontwikkeld waarbij aan de hand van zes functies van de financiële sector, verschillende clusters van ontwikkeling worden gedefinieerd.[9] Deze ontwikkelingen worden vervolgens mogelijk gemaakt door technologische krachten vanuit de maatschappij. Deze krachten worden hieronder verder besproken.

De verschillende clusters van ontwikkeling zijn volgens het WEF:

1. **Betalen:**
   a. de verdwijning van chartaal geld
   b. nieuwe betalingsnetwerken
2. **Verzekeren:**
   a. 'connected' verzekeren
   b. desaggregatie van verzekeringen
3. **Sparen en Lenen**
   a. verschuiven van klantbehoeftes
   b. alternatieve manier van lenen
4. **Het ophalen van kapitaal:**
   a. crowdfunding
5. **Investeringsmanagement:**
   a. proces externalisatie
   b. hogere betrokkenheid van investeerders
6. **Het faciliteren van data aan de markt:**
   a. nieuwe marktplatformen
   b. snellere en slimmere machines

Zie figuur 1 voor een overzicht.

8 Afgeleid van: www.investopedia.com/terms/r/regtech.asp, laatst geraadpleegd op 23 december 2016.
9 www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf, laatst geraadpleegd op 23 december 2016.



Figuur 1: Overzicht van functies, clusters en ontwikkelingen[10]

Vervolgens worden zes belangrijke ontwikkelingen geïdentificeerd die verschillende clusters verbinden:

1. meer gestroomlijnde infrastructuur;
2. automatisering van activiteiten met hoge kosten;
3. vermindering van tussenpersonen;
4. een strategische rol van data;
5. ontstaan van niches en gespecialiseerde producten;
6. meer betrokkenheid van klanten.

Deze ontwikkelingen zullen zich in meer of mindere mate 'cluster- en functie-overstijgend' manifesteren en worden gedreven door verschillende krachten die deze ontwikkelingen mogelijk maken.

10 www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf, laatst geraadpleegd op 23 december 2016.

Kijkend naar het voorbeeld van Achmea zien we dat FinTech zich manifesteert binnen de functie verzekeren, waar het in dit voorbeeld zich bevindt in het cluster 'connected' verzekeren. Deze sluit aan bij verschillende ontwikkelingen zoals een strategische rol van data en het ontstaan van niches en gespecialiseerde producten (autoverzekeringen voor voorzichtige rijders?). Deze ontwikkelingen worden vervolgens beïnvloed door krachten als gecomputeriseerde technologie en nieuwe toetreders (inspiratie kwam van buiten de sector), maar ook nieuwe privacywetgeving.

Krachten

Hieronder worden de krachten besproken die van invloed zijn op de bovengenoemde ontwikkelingen. Daarnaast zullen voorbeelden worden gegeven om deze invloed concreet weer te geven en wordt kort stilgestaan bij verschillende (risico/kans) scenario's die hieruit voortvloeien.

Kracht 1: Computertechnologie

De eerste 'kracht' is gecomputeriseerde technologie. De belangrijkste[11] zijn:

1. Blockchain
2. Big Data/Predictive Analytics
3. Artificial Intelligence (A.I.)/Machine learning
4. Biometrie (BioTech)
5. Application Programming Interface (API)
6. Open Source
7. Internet of Things (IoT)

In bijlage 1 worden deze technologieën kort toegelicht om een begrip te vormen van de werking.

De relevantie en invloed van deze technologieën op de integriteit van de financiële sector komt naar voren in de ontwikkelingen die hiermee gepaard gaan; bijvoorbeeld: 'de strategische rol van data'. Deze wordt gedreven door de mogelijkheden die big data en predictive analytics creëren. Vervolgens leidt het gebruik hiervan tot risico's en kansen voor de integriteit.

Het voorbeeld van Achmea betreft een dergelijk scenario. De verzekeraar liep met dit idee het risico op overtreding van (privacy)wetgeving, reputatieschade en druk op het

11 Technologieën die het meest naar voren komen in FinTech literatuur.

solidariteitsprincipe.[12] Hierdoor ontstaan ook ethische dilemma's en vraagstukken ten aanzien van inclusie en exclusie.[13]

Kracht 2: Nieuwe spelers ('start-ups' en 'BigTechs')

FinTech 'start-ups' zijn nieuwe organisaties die in feite ook vallen onder de definitie van technologie.[14] Deze 'vormen van organisatie' maken gebruik van kennis en gecomputeriseerde technologie (Kracht 1) en combineren deze opdat er een nieuw product (of dienst) ontstaat. Vervolgens kunnen zij deze aanbieden aan de markt of bestaande financiële ondernemingen. Het gebruik hiervan kan voor bestaande partijen nieuwe risico's en risicoscenario's met zich meebrengen. Bijvoorbeeld doordat deze start-ups zelf onvoldoende rekening hebben gehouden met de compliancevereisten.[15]

Wanneer start-ups producten/diensten direct aan de klant zullen gaan aanbieden, zullen zij in veel gevallen zelf over een vergunning van AFM of DNB moeten beschikken. Zie voor een verdere toelichting over vergunningen voor nieuwe spelers Kracht 4: Toezicht.

'BigTechs' zijn geen nieuwe organisaties, maar bestaande IT-organisaties die in eerste instantie niet bestaan om een functie binnen de financiële sector uit te oefenen. Zij hebben echter wel technologieën tot hun beschikking die mogelijk maken dat zich in die sector kunnen manifesteren. Voorbeelden daarvan zijn Facebook en Google. Zij hebben netwerken die zij met weinig aanpassingen kunnen gebruiken voor bijvoorbeeld betaaldienstverlening.[16] Deze partijen kunnen een bedreiging vormen voor de integriteit van de sector of bestaande organisaties die wellicht meer moeten concurreren. Ook wanneer BigTechs zelf de financiële sector betreden, zullen zij hun activiteiten moeten toetsen aan, en begrip hebben van integriteitsnormen die binnen de markt, sector of het land gelden. Zowel Facebook als Google begeven zich overigens al in de financiële sector.

12 "Dit beginsel ligt ten grondslag aan verzekeringen en houdt in dat een groot aantal leden van een groep verzekerden premie betalen waaruit de schade, die enkele van hen lijden, kan worden vergoed. De schade van enkelen wordt omgeslagen over de gehele groep." www.wftvragenbank.nl/, laatst geraadpleegd op 15 januari 2017. Echter, als mensen zich aan deze groep kunnen onttrekken en waarvan voorondersteld wordt dat zij minder risico zullen lopen (a.d.h.v. voorspellingen m.b.v. big data), wordt de premie voor zij die niet hun gegevens niet willen delen, of meer risico lopen hoger en misschien onbetaalbaar. Met name in de zorg kan dit voor ethische dilemma's/vraagstukken zorgen.

13 Federal Trade Commission, 'Big Data: A tool for inclusion or exclusion', 2016.

14 "Een systeem dat gebaseerd is op de toepassing van kennis, dat zich manifesteert in fysieke objecten en vormen van organisatie voor het behalen van bepaalde doelen."

15 Het overnemen van 'start-ups' door bestaande financiële ondernemingen en de risico's die hieraan verbonden zijn, kunnen wellicht ook worden meegenomen in een soort PARP. Vaak staat een 'start-up' vrijwel gelijk aan het product of de dienst die zij leveren. De manier waarop dit vorm gegeven kan worden valt echter buiten de reikwijdte van dit artikel.

16 www.emerce.nl/achtergrond/facebook-schuift-licentie-steeds-meer-richting-betalen, laatst geraadpleegd op 05 maart 2017.

Kracht 3: Wetgeving

De derde 'kracht' die zorgt voor een ontwikkeling in de sector is wetgeving. Een voorbeeld van internationale (Europese) wetgeving die technologische ontwikkeling beïnvloed, is de Payment Services Directive (PSD) 2.[17]

De PSD2 wordt door partijen aangegrepen om toe te treden tot de financiële sector (of zich aan te sluiten bij bestaande partijen[18]) en de consument te bedienen met nieuwe en/of verbeterde producten/diensten. Deze partijen zullen onder andere, met instemming van de consument, financiële gegevens kunnen gebruiken voor verschillende doeleinden, waaronder het verrichten van transacties onder mandaat van de consument. Deze ontwikkeling brengt nieuwe risico's en risicoscenario's met zich mee.[19]

Ook de Algemene Verordening Gegevensbescherming[20] (AVG) die op 25 mei 2018 in werking zal treden heeft impact op de benoemde ontwikkelingen. Daar waar data een strategische rol in gaat nemen en waar de infrastructuur meer gestroomlijnd wordt, dienen gegevens beschermd te worden wanneer deze zich verplaatsen, bewerkt en bewaard worden. De wijze waarop deze bescherming is bepaald in de AVG kan van invloed zijn op de activiteiten die een onderneming mag verrichten en kunnen evenals PSD2 nieuwe risico's en risicoscenario's met zich meebrengen ten aanzien van FinTech. Zo kan wetgeving, maar ook het toezicht daarop, een formalisatie zijn van een verschuivende norm in de samenleving en ethische dilemma's en vraagstukken blootleggen, die nog niet eerder expliciet in kaart werden gebracht.

Ook toekomstige wet- en regelgeving kan van invloed zijn. Bij het voorspellen van toekomstige wet- of regelgeving kan het helpen om de ethische vraagstukken in de maatschappij te bespreken en te kijken naar onderzoeken vanuit de overheid. Zo zal het ministerie van Binnenlandse Zaken onderzoek gaan doen naar mogelijkheden voor persoonlijk datamanagement.[21] En wilde minister Dijsselbloem graag 'afkijken' in Engeland en Duitsland.[22]

17 ec.europa.eu/finance/payments/framework/index_en.htm, laatst geraadpleegd op 14 januari 2017.
18 Dit kan bijvoorbeeld met behulp van technologie als API waarbij een derde partij een applicatie maakt voor consumenten om betaalrekeningen bij verschillende banken samen te voegen.
19 www.nporadio1.nl/nieuwsshow/onderwerpen/385503-bankgegevens-als-handelswaar, laatst geraadpleegd op 28 december 2016 en DNB onderzoeksrapport: 'Technologische innovatie en de Nederlandse financiële sector', 2016.
20 eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679, laatst geraadpleegd op 10 februari 2017.
21 www.binnenlandsbestuur.nl/digitaal/nieuws/onderzoek-naar-regie-over-eigen-gegevens-voor.9559090.lynkx, laatst geraadpleegd op 05 maart 2017.
22 www.rtlz.nl/tech/dijsselbloem-kijk-voor-fintech-ideeen-af-londen, laatst geraadpleegd op 05 maart 2017.

Kracht 4: Toezicht

Als laatste hebben ook toezichthouders invloed op technologische ontwikkelingen. Zij willen actief betrokken zijn bij deze ontwikkelingen en de risico's hiervan in kaart brengen. Hieraan ten grondslag ligt het idee dat meer concurrentie kan leiden tot betere en goedkopere producten en diensten.[23] Daarnaast willen zij blijvend kunnen voldoen aan de behoefte van de consument en maatschappij[24], alsmede een bijdrage leveren aan de concurrentiepositie (binnen en buiten de EU) en de reputatie van een land.

Een van de diensten die de Nederlandse toezichthouders hiervoor aanbiedt is de InnovationHub. Dit is een samenwerking van DNB en AFM die bedoeld is om *"nieuwe en bestaande innovatieve marktpartijen in de financiële sector met de toezichthouders in contact laten komen over vraagstukken op het gebied van financiële innovatie en regulering."*[25] Een verdere uitwerking hiervan is de 'Regulatory Sandbox', naar het idee van de FCA.[26] Deze Sandbox is *"een soort 'proeftuin' die neerkomt op een gecontroleerde omgeving voor het testen van innovatieve financiële producten en bedrijfsmodellen."*[27] Op deze manier proberen de toezichthouders (DNB/AFM) inzicht te vergaren in FinTech-ontwikkelingen en deze ontwikkelingen te accommoderen.[28]

Gezien de ontwikkelingen bij DNB en AFM ten aanzien van FinTech, blijkt dat zij zelf ook nog geen duidelijk zicht hebben op hoe deze technologische ontwikkelingen effect gaan hebben op de sector.[29] Daarnaast zien zij in dat regelgeving wellicht niet altijd verenigbaar is met het soort diensten/producten en nieuwe ondernemingen die willen toetreden. Dit kan voor zowel nieuwe als bestaande partijen risico's meebrengen voor de integriteit. Zo kan een bestaande partij een nieuwe dienst via de Sandbox uitproberen op de markt, terwijl de effecten hiervan op bijvoorbeeld 'klantbelang centraal' onzeker of onduidelijk zijn. Wellicht dat de toezichthouder situaties informeler en reactiever zal moeten benaderen, omdat zij geen gebruik kunnen maken van een duidelijk, wettelijk kader of eerdere ervaringen. Het gevolg daarvan kan informele handhaving zijn met een mogelijke onzekerheid voor marktpartijen.[30]

Wanneer er wordt gekeken naar een van de voorlopers op het gebied van toezicht en FinTech, de FCA, kan ook geconcludeerd worden dat toezichthouders graag zien dat

23 ACM: 'FinTech en concurrentie', 2016.
24 AFM en DNB: 'Meer ruimte voor innovatie in de financiële sector', 2016.
25 www.afm.nl/nl-nl/professionals/nieuws/2016/jun/innovation-hub, laatst geraadpleegd op 15 januari 2017.
26 Idem.
27 Idem.
28 www.dnb.nl/binaries/Toezicht%20Vooruitblik%202017_tcm46-349591.pdf, laatst geraadpleegd op 05 maart 2017.
29 Conclusie op basis van verschillende bronnen waaronder: Ter Braak en van de Ven, 'Hi Fin, I'm Tech! I'm here to take over…', *Jaarboek Compliance 2017*, Capelle ad IJssel: NCI.
30 fd.nl/opinie/1148627/toezichthouder-handhaaft-steeds-informeler, laatst geraadpleegd op 05 maart 2017.

RegTech gebruikt zal worden om compliance-activiteiten te automatiseren. Zo organiseerde de FCA al zogenaamde 'Hack-a-thons' die onder andere als doel had om geautomatiseerd advies te kunnen geven vanuit de toezichthouder.[31]

Een ander punt is de onduidelijkheid over de reikwijdte van het toezichtmandaat. Zo zit er bijvoorbeeld overlap in het toezicht tussen DNB/AFM enerzijds en de Autoriteit Persoonsgegevens (AP) anderzijds (met name bij de PSD2). Maar ook door het principe van ketenverantwoordelijkheid kunnen zowel de ACM als DNB/AFM-toezicht houden op de partijen die bij wijze van uitbesteding activiteiten verrichten voor ondernemingen die onder toezicht van DNB/AFM staan.[32] "Onvoorspelbaarheid van het toezicht vormt een niet te onderschatten gevaar voor de positie van de Nederlandse FinTech-sector."[33]

Combinaties

Uiteindelijk vormen de verschillende krachten weer een combinatie die van invloed is op de ontwikkelingen in FinTech, Een goed beeld over de verschillende krachten zal, wanneer deze gecombineerd worden, dan ook verschillende (toekomstige) kansen en risico's opleveren.

SIRA en FinTech

De relatie tussen FinTech en de SIRA kan vanuit twee perspectieven worden benaderd. Aan de ene kant kan FinTech zorgen voor een verandering in, of het ontstaan van nieuwe integriteitrisico's, maar aan de andere kant kan RegTech ook zorgen voor een verandering in de beheersing van integriteitrisico's. Hieronder zal worden besproken hoe de invloed van FinTech en RegTech in kaart kan worden gebracht, waarbij de focus van dit artikel ligt op risico-identificatie en -beheersing en de verwerking hiervan in de SIRA.

Deze methode zorgt ervoor dat een onderneming het volledige FinTech-spectrum (van toepassing op de onderneming) in acht kan nemen en toekomstige risico's voor de onderneming/sector kan definiëren. Dit laatste kan helpen bij de overweging voor ondernemingen om FinTech-oplossingen te overwegen. Wanneer niet eerst de verschillende ontwikkelingen worden besproken, kan men onbewust risico's/scenario's over het hoofd zien en een onvolledig beeld krijgen van de mogelijke kans en impact van een risico/

31 www.forbes.com/sites/tomgroenfeldt/2016/12/01/fca-promotes-regtech-to-bring-automation-to-compliance/#12d833cd104c, laatst geraadpleegd op 10 februari 2017.

32 Hoewel DNB/AFM formeel geen toezicht houden op deze partijen verwacht zij bijvoorbeeld van pensioenfondsen dat zij in hun uitbestedingscontract bedingen dat de toezichthouder rechtstreeks door de uitvoerder van informatie kan worden voorzien en de toezichthouder de mogelijkheid heeft om bij de uitvoerder ter plaatse onderzoek te doen of te laten doen. (DNB, Guidance: uitbesteding door pensioenfondsen, 2014).

33 fd.nl/opinie/1183405/onvoorspelbaarheid-van-toezicht-vormt-gevaar-voor-fintech-sector, laatst geraadpleegd op 10 februari 2017.

scenario. Wellicht dat in het voorbeeld van Achmea er op strategisch niveau andere keuzes waren gemaakt.

Een schematisch overzicht van de verschillende stappen:

Stap 1	Stap 2				Stap 3
Organisatieschets (functies)	**Categorie 1 (toekomst)**				**Categorie 1 (toekomst)**
• Cluster • Ontwikkelingen 1. 2. …	*Cluster/ontwikkeling*				
	Risico	Kans (tijd)	Kans	Impact	Bestaande beheersmaatregel
	Scenario (nieuw)				Nieuwe beheersmaatregel
					Nieuwe beheersmaatregel (RegTech, Stap 1)
	Categorie 2 (bestaand)				**Categorie 2 (bestaand)**
• Krachten 1. [Technologie] 2. [Nieuwe spelers] 3. [Wetgeving} 4. [Toezichthouders] [Combinaties]	*Cluster/ontwikkeling*				
	Risico	Kans	Impact		Bestaande beheersmaatregel
	Scenario (oud, aanpassing)				Nieuwe beheersmaatregel
					Nieuwe beheersmaatregel (RegTech, Stap 1)
	Cluster/ontwikkeling				
	Risico	Kans	Impact		Bestaande beheersmaatregel
	Scenario (nieuw)				Nieuwe beheersmaatregel
					Nieuwe beheersmaatregel (RegTech, Stap 1)

Stap 1: Organisatieschets

Cluster – FinTech-ontwikkeling

Voordat risico's en scenario's gedefinieerd worden, is het belangrijk om te schetsen waar de onderneming zich in de sector bevindt. Bepaal in welke clusters de onderneming zich bevindt en welke ontwikkelingen hierbij van invloed kunnen zijn op de onderneming. Deze ontwikkelingen zijn in feite ook algemene scenario's van waaruit risicoscenario's gedefinieerd kunnen worden wanneer deze als blauwdruk onder de activiteiten van de onderneming worden gelegd. In dat geval gaat het om toekomstige scenario's (categorie 1, zie stap 2).

Definieer vervolgens de verschillende krachten met behulp van actuele informatie. Verzamel hiervoor zoveel mogelijk relevante informatie en gebruik daarbij de kennis van 'betrokken partijen' (zie: Uitwerking).

Stap 2: Risico-identificatie en analyse

Risico - Scenario

Hier wordt het risico voor de onderneming of sector gedefinieerd en worden scenario's beschreven. Daarbij kan worden gekeken naar risico's die op dit moment reëel zijn, maar ook naar toekomstige risico's en de manier waarop deze zich zullen manifesteren. Hoewel dit wellicht voor verwarring zorgt is het belangrijk dit te bespreken. Een voorbeeld hiervan is het scenario dat robots een gevaar worden voor de mensheid, omdat zij hun eigen wil hebben ontwikkeld.

Loop hierbij langs de verschillende krachten die invloed hebben op de ontwikkelingen binnen de clusters waar de onderneming actief is. Bepaal bij elke kracht of deze zorgt voor een nieuw risico/scenario, of de aanpassing van een bestaand risico/scenario en op welke wijze dit het risico of het scenario beïnvloedt.

Kans

Bij het onderdeel kans wordt er onderscheid gemaakt tussen FinTech-ontwikkelingen die nog niet geïmplementeerd zijn in de onderneming (categorie 1) en ontwikkelingen die dit wel zijn (categorie 2). Eventueel kan ook een derde categorie worden gemaakt met FinTech-ontwikkelingen die nog niet gerealiseerd zijn in de sector.

In het geval van categorie 1 ontwikkelingen wordt kans bepaald door te veronderstellen dat deze ontwikkelingen zich wel gemanifesteerd hebben. Daarnaast wordt een inschatting gemaakt van wanneer deze ontwikkeling zich gaat manifesteren. Zo ontstaan er twee dimensies aan de hand waarvan de kans voor categorie 1 ontwikkelingen wordt bepaald. Zo kan bij het voorbeeld van technologische singulariteit de kans groot zijn, maar lijkt het erop dat een dergelijk scenario pas over 10 jaar realistisch is. Een bruikbaar instrument voor het bepalen van de tijdsfactor is de 'hype cycle' van Gartner[34]. Gartner doet onderzoek naar innovaties en bepaalt de status van deze innovaties met uiteindelijk de fase van acceptatie door de markt. Eventueel kan de tijdsfactor gebruikt worden om de kans op het risico te 'verdisconteren'. In het geval van categorie 2 ontwikkelingen kan worden volstaan met het bepalen van de kans aan de hand van één dimensie (zoals ook in de guidance van DNB wordt beschreven[35]).

34 www.gartner.com/technology/research/methodologies/hype-cycle.jsp, laatst geraadpleegd op 23 december 2016.

35 DNB, 'De integriteit-risicoanalyse', 2015.

De aanpak zoals hier wordt beschreven kan ook gebruikt worden om integriteitrisico's bij de ontwikkeling van nieuwe producten/diensten van de onderneming in kaart te brengen tijdens het PARP.

Loop bij het bepalen van elke kans elke kracht na en kijk of en in hoeverre deze impact heeft op de kans.

Impact

Bij het bepalen van de impact van huidige/toekomstige risico's/scenario's op het gebied van FinTech kan worden gekeken naar de algemene tendens binnen de maatschappij en bij de toezichthouder. Voor FinTech zal er weinig jurisprudentie bestaan ten aanzien van handhaving door de toezichthouder, wellicht dat voor specifieke risico's/scenario's al uitspraken bestaan van toezichthouders in het buitenland. Zo heeft de Duitse toezichthouder zich twee jaar geleden al uitgelaten over 'video-onboarding'[36] en waarschuwt de AFM voor toekomstig misbruik van de PSD2[37]. Daarnaast heeft DNB in haar visiedocument over FinTech[38] een algemene inschatting van de impact van FinTech op de sector gegeven (zie figuur 2). Ook de tendens in de maatschappij kan worden gemonitord. Wanneer het bijvoorbeeld gaat over persoonsgegevens geeft onderzoek aan dat jongeren de BigTech-bedrijven als Google en Facebook sterk wantrouwen.[39]

36 www.bbvaresearch.com/wp-content/uploads/2016/02/Financial-Regulation-Outlook_Feb_2016_Cap 10.pdf, laatst geraadpleegd op 05 maart 2017.

37 nos.nl/artikel/2145844-afm-vreest-misbruik-als-banken-klantgegevens-gaan-delen.html, laatst geraadpleegd op 05 maart 2017.

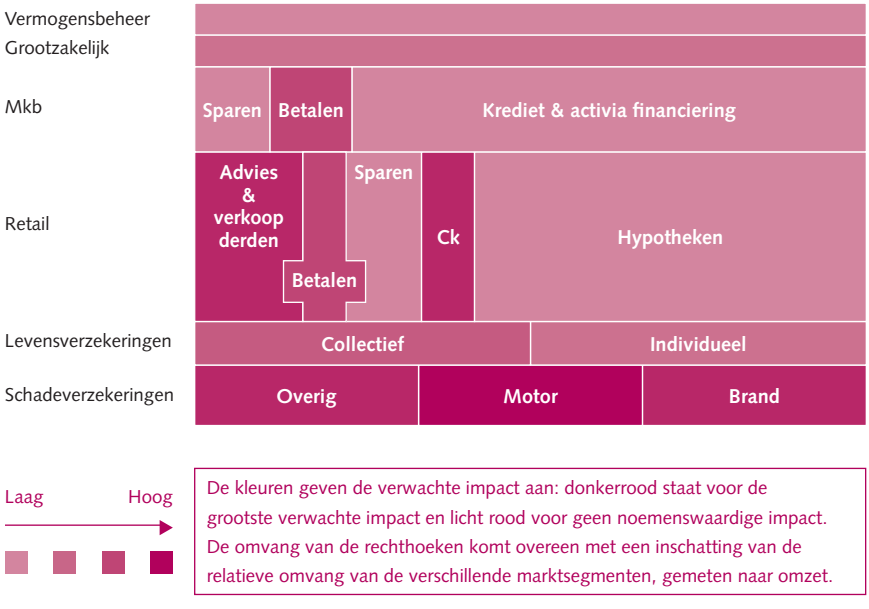
38 DNB, 'Technologische innovatie en de Nederlandse financiële sector', 2016.

39 jij.eenvandaag.nl/uitslagen/69830/jongeren_vertrouwen_facebook_en_google_niet, laatst geraadpleegd op 05 maart 2017.

Box 3 Basisscenario verwachte impact op omzet Nederlandse financiële sector in 2020

Figuur 2 geeft een ruwe inschatting (op basis van lineaire extrapolatie) van de impact van technologische innovatie op de verschillende marktsegmenten in de financiële sector over de komende vijf jaar, waarbij de stand van zaken (lees: de mate van innovatie) in 2015 als uitgangspunt dient. Voor de komende vijf jaar wordt de grootste impact verwacht in het financieel advies, het consumentenkrediet (CK) en de autoverzekeringen. Ook voor betaaldiensten en overige schadeverzekeringen wordt een aanzienlijke impact verwacht. Bijbetaaldiensten is innovatie al relatief ver ontwikkeld, waardoor de toekomstige impact in vergelijking met de impact vandaag kleiner is dan bij bijvoorbeeld financieel advies. Bij de inschatting is alleen gebruik gemaakt van een lineaire extrapolatie van reeds bestaande ontwikkelingen. Eventuele effecten van de tweede orde, zoals cross-selling bij betaaldiensten, zijn niet meegenomen.

Impact technologische innovatie (lineaire inschatting)



Figuur 2: Overzicht van algemene impact FinTech-ontwikkelingen op de sector[40]

40 DNB, 'Technologische innovatie en de Nederlandse financiële sector', 2016.

Stap 3: Risicobeheersing

In het geval van risicobeheersing wordt gekeken naar de verschillende beheersmaatregelen die de gestelde risico's kunnen beheersen. Zoals besproken kan RegTech zorgen voor invloed op bestaande beheersmaatregelen, maar ook mogelijkheid bieden tot nieuwe beheersmaatregelen.

Conform Stap 1, kunnen ook de RegTech-ontwikkelingen worden geïdentificeerd en gedefinieerd.

Zo kunnen niet-integere transacties 'real time'[41] gemonitord en bijgestuurd worden[42] en gebruikt JP Morgan een algoritme om het gedrag van handelaren te monitoren.[43] Al deze data kan vervolgens ook gebruikt worden om (middels algoritmes) voorspellingen te doen van gedrag van medewerkers om risico's vroegtijdig te identificeren (profiling[44]). Profiling levert daarbij wel andere bezwaren op. Zo kan het algoritme onjuiste conclusies trekken die leiden tot discriminatie en racisme.[45]

Uit onderzoek van het Institute of International Finance blijkt dat RegTech in ieder geval kan zorgen voor verbeteringen op onder andere onderstaande onderdelen:

1. het verzamelen en bundelen van grote hoeveelheden data;
2. scenario analyse en het doen van voorspellingen;
3. real-time transacties monitoren;
4. identificatie van klanten en rechtspersonen;
5. het monitoren van gedrag en cultuur binnen de onderneming;
6. monitoren en interpreteren van nieuwe wetgeving.[46]

Een mogelijkheid waarbij RegTech ook integriteitrisico's kan beheersen, is wanneer bepaalde technologieën worden gebruikt door de toezichthouder welke vroegtijdig lacunes in gebruikelijke beheersmaatregelen binnen de sector kan opsporen en deze deelt met de verschillende financiële ondernemingen. Bijvoorbeeld de mogelijkheid om de

41 Realtime interactie vindt plaats zonder vertragingen of wachttijden als gevolg van de verwerking van gegevens, www.encyclo.nl/begrip/Realtime, laatst geraadpleegd op 12 februari 2017.

42 www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/Managing_your_business/GC-Transaction-Monitoring.pdf, laatst geraadpleegd op 12 februari 2017.

43 www.bloomberg.com/news/articles/2015-04-08/jpmorgan-algorithm-knows-you-re-a-rogue-employee-before-you-do, laatst geraadpleegd op 05 maart 2017.

44 autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-en-tv/profiling, laatst geraadpleegd op 05 maart 2017.

45 www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing, laatst geraadpleegd op 12 februari 2017.

46 www.iif.com/publication/research-note/regtech-financial-services-solutions-compliance-and-reporting, laatst geraadpleegd op 05 maart 2017.

effectenhandel stop te zetten naar aanleiding van fraude die met RegTech door de toezichthouder vroegtijdig is gesignaleerd.

Verwerking in de SIRA

Wanneer bovenstaande methode is toegepast ontstaat een overzicht van de mogelijke integriteitrisico's die FinTech-ontwikkelingen met zich mee kunnen brengen. Deze dienen vervolgens in de SIRA verwerkt te worden. Per risico zal het scenario uitwijzen welke van de integriteitthema's de ontwikkeling zal raken (bijvoorbeeld: belangenverstrengeling en fraude). Op deze wijze kan het scenario worden onderverdeeld in de SIRA. Daarbij kan onderscheid worden gemaakt tussen nieuwe risico's/scenario's en bestaande risico's/scenario's die veranderen door deze ontwikkeling(en).

Ook ontstaat door bovenstaande methode een overzicht van de mogelijke invloed van FinTech op de beheersmaatregelen van de onderneming. Deze maatregelen kunnen verdeeld worden onder maatregelen die invloed hebben op bestaande risico's, nieuwe risico's, maar ook op bestaande beheersmaatregelen.

Het is van belang om bij het verwerken van het bovenstaande de volgende vragen te beantwoorden:

1. Betreft het een nieuw risico?
2. Betreft het de aanpassing van een bestaand risico?
3. Betreft het een nieuw scenario van een nieuw risico?
4. Betreft het een nieuw scenario van een bestaand risico?
5. Betreft het een nieuwe beheersmaatregel voor een nieuw risico/scenario?
6. Betreft het een nieuwe beheersmaatregel voor een bestaand risico/scenario?
7. Heeft deze nieuwe beheersmaatregel ook invloed op andere bestaande/nieuwe risico's/scenario's?
8. Op welk integriteitthema heeft het invloed?

De antwoorden op deze vragen kunnen vervolgens worden verwerkt door deze in de SIRA te plaatsen.

Uitwerking

Betrokken partijen

Voor het uitwerken van risico's/scenario's en het bepalen van kans en impact is het belangrijk dat de juiste partijen aanwezig zijn.[47] In het geval van FinTech is het belangrijk dat er specialisme aanwezig is op het gebied van gecomputeriseerde technologie, bijvoorbeeld de chief information officer en andere IT medewerkers. Ook is het goed

47 In het algemeen kan een stakeholder analyse een goede uitkomst bieden voor het zoeken naar partijen die relevante informatie kunnen leveren voor de SIRA.

om bij het bespreken van ontwikkelingen die zich in de toekomst gaan manifesteren de mogelijkheid te onderzoeken om betrokkenheid van de toezichthouder te vragen via de InnovationHub[48]. Wellicht dat er in de toekomst ook onafhankelijk toezicht komt op data door een soort custodian. Die kan zowel intern over de organisatie toezicht houden, als over een netwerk van organisaties die dezelfde data gebruiken. Zij zouden betrokken kunnen worden en inzichtelijk kunnen maken of het gebruik van data aan gestelde normen en waarden voldoet.[49]

Loop de verschillende krachten langs en inventariseer welke (externe) partijen betrokken kunnen worden bij de uitwerking.

Uitgangspuntendocument

De wijze waarop deze analyse wordt georganiseerd, welke definities worden gehanteerd, wie er betrokken zijn, welke schalen er voor kans en impact worden gebruikt en overige uitgangspunten worden beschreven in het uitgangspuntendocument. Deze geeft begeleiding aan het analysemodel.

De casus Achmea - uitgewerkt

Zonder uitgangspuntendocument of betrokkenheid van de juiste partijen wordt de hierboven beschreven methode ter illustratie, gedeeltelijk toegepast op eerdergenoemde casus van Achmea.

Stap 1:

Zoals eerder beschreven zien we dat in de casus van Achmea FinTech zich manifesteert binnen de functie verzekeren, waar het in dit voorbeeld zich bevindt in het cluster 'connected' verzekeren. Deze sluit aan bij verschillende ontwikkelingen zoals een strategische rol van data en het ontstaan van niches en gespecialiseerde producten (autoverzekeringen voor voorzichtige rijders?). Deze ontwikkelingen worden vervolgens beïnvloed door krachten als gecomputeriseerde technologie en nieuwe toetreders (inspiratie kwam van buiten de sector), maar ook nieuwe privacywetgeving.

Stap 2:

Een scenario dat zich voordoet is dat een groot deel van de klanten van Achmea tegen korting wel, en een klein deel niet mee wil doen aan deze vorm van verzekeren. Het gevolg hiervan kan zijn dat klanten toch gedwongen worden hun data te delen, omdat zij anders een te groot risico opleveren, wat zich vertaald in een hoge

48 www.dnb.nl/toezichtprofessioneel/innovationhub, laatst geraadpleegd op 12 februari 2017.

49 Naar een idee van KPMG: fd.nl/opinie/1187276/onafhankelijk-toezicht-nodig-op-het-toepassen-van-data-in-systemen, laatst geraadpleegd op 13 februari 2017.

premie die deze klanten niet kunnen betalen en Achmea steeds minder het solidariteitsprincipe in acht kan nemen. De kans dat dit zich voordoet wordt beïnvloed door de mate waarin klanten hun data delen voor korting. Zonder onderbouwing kan die kans gezien ons gedrag ten aanzien van algemene voorwaarden worden vastgesteld op hoog. De impact van dit risico zit grotendeels in reputatieschade. Het is niet per sé verboden. Hoe de impact vastgesteld kan worden wordt overgelaten aan de lezer.

Een ander (categorie 1, toekomstig) scenario is dat Achmea deze data combineert met betaalgegevens (verkregen via de PSD2) en een algemeen risicoprofiel ontwikkeld ('profiling') dat zorgt voor een groep van klanten die qua risico in de categorie 'onverzekerbaar' terecht komen. De kans dat dit gebeurt versterkt naarmate de implementatie van PSD2 dichterbij komt. Daarbij is de kans dat klanten naast hun rijgedrag ook best hun betaalgedrag willen prijsgeven voor korting. De impact hiervan wordt bepaald door een verschuivende norm ten aanzien van privacy en een actieve AP, alsmede AFM die deze activiteit wellicht kunnen beoordelen als niet in het belang van de klant en schadelijk voor het solidariteitsbeginsel en de maatschappij. Daarnaast kan hier ook reputatieschade ontstaan, mede door de ontwikkeling van de mondige, kritische consument die (via sociale media) steeds meer publiek weet te bereiken.

Stap 3:
Technologie en verscherpte wetgeving kunnen er ook voor zorgen dat er beheersmaatregelen ontstaan. Zo kan Achmea ervoor kiezen om een bepaalde buffer in te programmeren die ervoor zorgt dat incidenten niet meetellen als consequent slecht rijgedrag. Ook kan een algoritme met de opdracht "bewaak het solidariteitsbeginsel" toch zorgen voor een betaalbare premie voor beide groepen verzekerden. Ook kan een toezichthouder of wetgever voorschrijven dat een privacy officer voldoende kennis moet hebben van algoritmes om de integriteitrisico's op dit punt te bewaken. Daarnaast zorgen bestaande beheersmaatregelen zoals privacybeleid al voor een bepaalde mate van beheersing.

Verwerking in de SIRA:
De beschreven scenario's hebben invloed op het integriteitthema zorgplicht en maatschappelijk onbetamelijk gedrag en het specifieke risico dat Achmea niet voldoet aan haar zorgplicht richting de klant, met als gevolg dat het belang van de klant niet centraal gesteld wordt.

Het zijn nieuwe scenario's die invloed hebben op een bestaand risico. Daarbij kunnen zowel nieuwe als bestaande beheersmaatregelen nu en in de toekomst zorgen voor adequate risicobeheersing. Doordat ook naar een toekomstig scenario is gekeken kan Achmea er ook voor kiezen om een dergelijk initiatief toch niet in de markt te zetten.

Conclusie

In dit artikel is getracht antwoord te geven op de vragen: Wat is de invloed van FinTech op integriteitrisico's in de financiële sector, en hoe kan dit worden verwerkt in de SIRA? Daarbij was het doel om voor compliance officers een methode te beschrijven aan de hand waarvan FinTech-ontwikkelingen binnen de financiële sector en ondernemingen benaderd kunnen worden en de integriteitrisico's die hier mogelijk uit voortvloeien geanalyseerd kunnen worden. Daarnaast is besproken op welke wijze FinTech integriteitrisico's kan beheersen. In dit geval wordt er ook wel gesproken van RegTech.

Met behulp van een overzicht van clusters van innovatie, welke verschillende functies van de financiële sector overstijgen en waar verschillende ontwikkelingen aan ten grondslag liggen, kan de onderneming bepalen in welke situatie zij zich bevindt en welke FinTech-ontwikkelingen zich binnen de onderneming en in de markt afspelen. Vervolgens kunnen huidige en toekomstige FinTech-risico's en -scenario's binnen de onderneming en in de sector worden geïdentificeerd en gedefinieerd. Tijdens dit proces zorgt het toetsen aan de verschillende krachten die de FinTech-ontwikkelingen drijven voor een juiste identificatie en definiëring. Deze krachten moeten gemonitord worden om te kijken in hoeverre actuele informatie over deze krachten bekend is. Hierbij kan gebruik worden gemaakt van de kennis van betrokken partijen. Wanneer niet eerst de verschillende ontwikkelingen worden besproken kan men onbewust risico's/scenario's negeren, en een onvolledig beeld krijgen van de mogelijke kans en impact van een nieuw of bestaand, maar aangepast risico/scenario.

Bij het bepalen van het onderdeel kans moet een onderscheid worden gemaakt tussen toekomstige (zgn. categorie 1) en huidige (zgn. categorie 2) ontwikkelingen. Daarbij wordt in de eerste categorie een extra dimensie van tijd toegevoegd aan het onderdeel kans. Deze categorie kan ook worden gebruikt bij de ontwikkeling van nieuwe producten/diensten en/of organisatievormen. In dat geval is deze methode ook bruikbaar voor het PARP en kan het helpen bij de overweging voor ondernemingen om FinTech-oplossingen te implementeren/over te nemen. Vervolgens dienen de uitkomsten van deze analyse verwerkt te worden in de SIRA. Hiervoor is een set aan vragen opgesteld. Een eerste poging voor de toepassing van deze methode is verricht met behulp van het voorbeeld van Achmea.

Wanneer een onderneming een dergelijke analyse opstelt is het belangrijk om daarbij de uitgangspunten vast te leggen en de juiste partijen en informatiebronnen (intern en extern) te betrekken. Hiervoor zijn een aantal voorbeelden gegeven. Dit kan worden getoetst door de verschillende krachten langs te lopen.
Door deze methode te hanteren kan door de onderneming uiteindelijk worden bepaald hoe FinTech invloed heeft op het analyseren van integriteitrisico's die de onderneming loopt, maar ook hoe RegTech integriteitrisico's kan beheersen. Wat hieruit blijkt is dat FinTech op zich geen integriteitrisico is, maar dat deze wel invloed heeft op de integriteit-

thema's zoals deze in de SIRA zijn benoemd. Hierbij lijkt FinTech op het thema gedrag & cultuur, ook dit zit verweven in de verschillende integriteitthema's.

Beperkingen

Een beperking aan dit artikel is dat een dergelijke exercitie nog niet daadwerkelijk heeft plaatsgevonden en deze methode daarom nog niet in praktijk is getoetst. Daarnaast is de methode algemeen beschreven en dient er een vertaalslag plaats te vinden om deze toe te kunnen passen op een specifieke onderneming. Ook kan er verwarring ontstaan doordat er verschillende termen worden gebruikt om ontwikkeling te duiden (clusters, krachten, ontwikkelingen). Dit komt doordat de methode is ontwikkeld voor zowel bestaande als toekomstige FinTech- integriteitrisico's en beheersmaatregelen.

De vraag van de consument, c.q. het consumentengedrag en hoe deze van invloed is op de sector wordt in dit artikel niet gedefinieerd als kracht, maar als ontwikkeling. De reden is dat wordt uitgegaan van het principe dat de verschillende krachten invloed hebben op deze vraag en deze zich niet autonoom ontwikkelt. De inherente complexiteit van de financiële sector en de informatie-asymmetrie lijken dit uitgangspunt te ondersteunen. Er wordt dus uitgegaan van een consument die zonder voldoende informatie en ondersteuning (vanuit wet- en regelgeving en de toezichthouders) geen autonome en juiste keuzes kan maken.[50]

Openstaande actiepunten

Zoals hierboven besproken dient deze methode te worden getoetst in de praktijk. Dit kan per onderneming worden gedaan, maar ook met verschillende ondernemingen. Dit lijkt op de wijze waarop de regulatory sandbox[51] is opgezet. Daarbij kunnen ook externe partijen worden betrokken, waaronder de relevante ministeries, toezichthouders, nieuwe toetreders, tech.-ondernemingen en kennisinstituten. Een bijkomend voordeel is dat betrokken partijen normen kunnen definiëren die worden gesteld aan bepaalde toekomstige FinTech-ontwikkelingen.

Afsluiting

Ter afsluiting en ter begrip van de wijze waarop er naar FinTech moet worden gekeken volgt de volgende quote van Sir Mark Walport (UK Government Chief Scientific Adviser): *"Like any technology, FinTech is neither good nor bad in itself. It is the specific uses of the technology that can be good or bad."*[52]

50 Awww.afm.nl/~/profmedia/files/thema/thema-kbc/kbc-verhaal-printversie2.ashx, laatst geraadpleegd op 05 maart 2017.

51 www.afm.nl/nl-nl/professionals/nieuws/2016/dec/maatwerk-innovatie, laatst geraadpleegd op 05 maart 2017.

52 www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf, laatst geraadpleegd op 05 maart 2017.

Bijlage 1

Definities van genoemde technologieën onder 'Kracht 1':

1. Blockchain

"Om eenvoudig uit te leggen wat een blockchain nu is kan deze vorm van databeheer het beste worden vergeleken met een spreadsheet of een excel werkblad. Het universele grootboek van de blockchain is niets anders dan een lijst zoals in een spreadsheet. Een excelsheet die is gedeeld met iedereen ter wereld. Een lijst met gegevens waarbij iedereen die meedoet een exacte kopie van die lijst krijgt en kan zien wat er in staat. Iedereen met de spreadsheet kan vervolgens ook wijzigingen aanbrengen in de database. En wanneer een wijziging in de spreadsheet wordt gemaakt, dan wordt deze aanpassing direct overgenomen op alle andere kopietjes van de lijst. Het resultaat is dat iedereen altijd naar dezelfde lijst met gegevens kijkt. Overal ter wereld. Mensen die google drive gebruiken weten dat dit soort spreadsheets al bestaan met de mogelijkheid om de google sheets te delen. Er is echter één eigenschap die blockchains uniek maakt. En dat is dat aan een blockchain alleen nieuwe regels toegevoegd kunnen worden aan de onderkant van de lijst. In feite is hiermee het enige wat een blockchain doet het toevoegen van nieuwe rijen, die automatisch met iedereen worden gedeeld. Het is niet mogelijk om een wijziging door te voeren in eerder toegevoegde regels. De cryptografische software zorgt hier voor, door het combineren van alle rekenkracht in het netwerk voor de controle van de toevoegingen en het weigeren van mutaties."[53]

2. Big Data/predictive analytics

"Big Data wordt vooral gebruikt om correlaties te vinden tussen fenomenen, personen en gebeurtenissen. Op basis van die correlaties worden vervolgens beslissingen genomen. (…) Big Data bevat twee componenten. Allereerst de computertechnologie: de steeds geavanceerder hard- en software die het mogelijk maakt meer data te verzamelen, te bewerken en te bewaren. Het tweede component is de statistiek die het mogelijk maakt om in een verzameling losse data betekenis te vinden. (…) De twee componenten van big data (hard- en softwarecapaciteiten en statistiek) leiden tot een explosie van nieuwe toepassingen op het gebied van zogenoemde predictive analysis – dus: toekomstvoorspellingen."[54]

"Predictive analytics is een term die gebruikt wordt om een serie analytische statistische technieken te beschrijven die gebruikt worden om toekomstige acties en gedragingen te kunnen voorspellen. In business wordt predictive analytics gebruikt om proactieve beslissingen te kunnen maken en acties te bepalen. Predictive analytics maakt gebruik

53 www.watisblockchain.nl/wat_is_blockchain.php, laatst geraadpleegd op 15 januari 2017.
54 decorrespondent.nl/296/wat-is-big-data/14414312-a609db7d, laatst geraadpleegd op 15 januari 2017.

van statistische modellen om patronen in historische- en transactionele data te ontdekken om zowel risico's als kansen bloot te leggen."[55]

3. Artificial intelligence (A.I.) / Machine learning

"A.I., oftewel kunstmatige intelligentie laat computers zich zo gedragen dat het intelligent zou heten als mensen het op die manier zouden doen."[56] Intelligentie wordt daarbij gedefinieerd als: *"Het geheel van cognitieve of verstandelijke vermogens dat nodig is om kennis te verwerven en daar op een goede wijze gebruik van te maken, teneinde problemen op te lossen die een vast omschreven doel en structuur hebben."*[57]
Machine learning is een vorm van A.I. die computers het vermogen geeft om te leren van bestaande en nieuwe data zonder hiervoor vooraf expliciet geprogrammeerd te zijn.[58]

4. Biometrie (BioTech)

"Met de term biometrie wordt gedoeld op het herkennen van mensen aan een lichaamskenmerk met gebruikmaking van informatietechnologie. Als de identiteit van mensen gecontroleerd wordt met behulp van een pasfoto of een signalement, spreken we doorgaans niet van biometrie. Wel als deze controle geautomatiseerd plaatsvindt. Informatietechnologie maakt het tegenwoordig mogelijk lichaamskenmerken snel te digitaliseren om ze vervolgens óf te kunnen afbeelden, óf om er berekeningen op los te laten. Dat kan bijvoorbeeld met de omtrek van de hand of een vinger, de afdruk van een vinger of met het patroon van de iris. Zelfs veranderlijke lichaamskenmerken zijn voor biometrische persoonsherkenning bruikbaar, zoals de stem, de schrijfbeweging bijvoorbeeld wanneer men zijn handtekening zet, of het ritme waarin men bepaalde woorden typt op een toetsenbord."[59]

5. Application Programming Interface (API)

"Een API is een set aan definities waarmee softwareprogramma's onderling kunnen communiceren. Het dient als een interface tussen verschillende softwareapplicaties waardoor de gebruikte code automatisch elkaar toegang tot informatie en/of functionaliteit geeft, zonder dat ontwikkelaars hoeven te weten hoe het andere programma exact werkt."[60]

55 www.analyticstoday.nl/kennis/wat-is-predictive-analytics-en-wat-zijn-de-voordelen, laatst geraadpleegd op 15 januari 2017.
56 Walter Kosters, Universiteit Leiden: liacs.leidenuniv.nl/~kosterswa/AI/aieen.pdf, laatst geraadpleegd op 15 januari 2017.
57 Resing en Drenth, 'Intelligentie: weten en meten' 2009.
58 Naar: whatis.techtarget.com/definition/machine-learning, laatst geraadpleegd op 15 januari 2017.
59 Grijpink, 'Biometrie en privacy'. *Privacy & Informatie*, 2000.
60 computerworld.nl/development/74796-wat-is-een-api, laatst geraadpleegd op 15 januari 2017.

6. Open Source

"Open source software is software waarvan de broncode is gepubliceerd en vrij beschikbaar is voor het publiek. Iedereen kan op die manier vrij kopiëren, aanpassen en verspreiden zonder kosten aan auteursrechten en toeslagen. De ontwikkeling van open source software gebeurt door gemeenschappelijke samenwerking van zowel individuele programmeurs als grote bedrijven."[61]

7. Internet of things (IoT)

"De interconnectiviteit van 'alledaagse objecten' die via het internet in staat zijn data te zenden en ontvangen door computers die daarin verwerkt zijn."[62]

61 www.transip.nl/vragen/322-wat-is-open-source-software, laatst geraadpleegd op 15 januari 2017.
62 Naar: en.oxforddictionaries.com/definition/Internet_of_things, laatst geraadpleegd op 15 januari 2017.