Ontketend

Toezicht op een open bankensector

DeNederlandscheBank
EUROSYSTEEM

Inhoudsopgave

1 Inleiding

De bancaire sector wordt meer open. Gedreven door onder meer technologische innovatie en veranderende regelgeving treden nieuwe partijen toe tot de financiële sector en daarmee verandert het speelveld voor gevestigde banken. Banken bedienen steeds minder de gehele waardeketen van productontwikkeling tot eindklant. Diverse partijen bieden onderdelen van deze keten aan en werken op verschillende manieren samen met de traditionele banken.

In deze publicatie analyseert De Nederlandsche Bank (DNB) de gevolgen van een meer open banken sector voor het prudentiële en integriteitstoezicht. Dit sluit aan op één van de drie speerpunten uit de Visie op Toezicht 2018-2022, namelijk “Inspelen op technologische vernieuwing”.

DNB ziet voordelen in de ontvlechting van waardeketens en grotere openheid, omdat hierdoor innovaties kunnen opbloeien en de efficiëntie van financiële dienstverlening toeneemt. Tegelijkertijd vindt DNB het van groot belang dat deze openheid niet leidt tot onduidelijkheid over verantwoordelijkheden. Ook in meer open, langere en soms complexere ketens blijven onder toezicht staande instellingen (en bestuur) verant-woordelijkheid dragen. Zij zijn verantwoordelijk voor hun producten en dienstverlening aan de consument, ook als ze onderdelen hiervan uitbesteden of hiervoor samenwerken met derde partijen.

Het volgende hoofdstuk legt uit welke vormen een open bankensector kan aannemen. Hoofdstuk 3 zet uiteen welke gevolgen een steeds opener bankensector heeft voor banken, waarbij gekeken wordt naar opeenvolgend de operationele bedrijfsvoering, de beheersing van integriteitsrisico’s en het verdienmodel. Hoofdstuk 4 gaat in op de gevolgen voor het financieel systeem als geheel, waarbij we zowel de kansen als de risico's belichten. Het laatste hoofdstuk behandelt de verwachtingen ten aanzien van de sector en de vervolg-stappen voor het toezicht van DNB.

2 Open bankensector

2.1 Openheid van de waardeketen

De bankensector wordt meer open.[1] Openheid speelt op twee fronten, in de waardeketens (verticaal) en in de interactie met de klant (horizontaal).

Banken ontvlechten hun waardeketen (verticaal). Bancaire waardeketens bestaan uit verschillende procesonderdelen en lopen van de ondersteunende back office-diensten en productontwikkeling tot de uiteindelijke verkoop aan de consument. Banken nemen niet vanzelfsprekend de gehele waardeketen voor hun rekening. Steeds vaker treden derde partijen toe, waaronder fintechs en IT-bedrijven, die een onderdeel van de waardeketen van de bank verzorgen via een uitbesteding.

Tevens werken banken met derde partijen samen om nieuwe, innovatieve diensten te ontwikkelen.

Banken beheren minder vanzelfsprekend de interactie met hun klant (horizontaal). Met bijvoorbeeld nieuwe apps kunnen consumenten via één partij een overzicht van al hun rekeningen bij verschillende banken krijgen. Daarnaast zetten banken stappen om bancaire diensten in de toekomst ook via platforms te organiseren, waarbij vragers en aanbieders virtueel bij elkaar worden gebracht en een bank ook (concurrerende) producten van derden aanbiedt. Figuur 1 laat gestileerd zien hoe de verticale ontvlechting en de horizontale verschuiving rondom het klantcontact er uitziet voor kredietverlening.

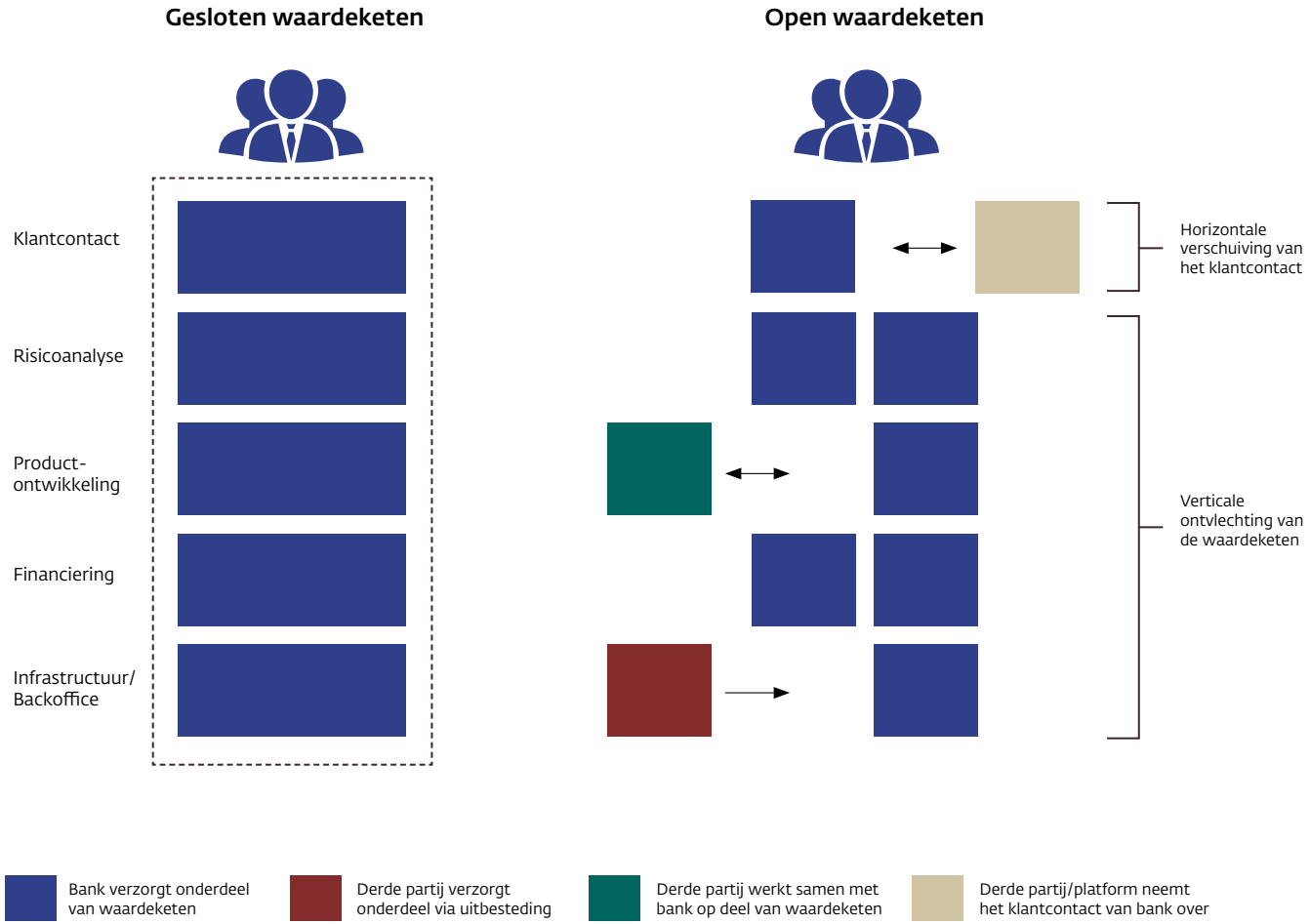
2.2 Openheid via uitbestedingen

Uitbestedingen zijn in toenemende mate van wezenlijk belang voor de bedrijfsvoering van banken. Europese banken spenderen grofweg 42% van hun IT-budget aan uitbestedingen aan derde partijen tegenover 35% vijf jaar geleden, zo blijkt uit ECB-onderzoek. Waar in eerste instantie ondersteunende diensten werden uitbesteed, zoals HR-administratie en marketingactiviteiten, worden nu steeds vaker materiële activiteiten uitbesteed die dichter op het kernbedrijf zitten. Deels wordt dit mogelijk gemaakt door nieuwe typen van uitbestedingen, die aan een opmars bezig zijn mede dankzij technologische vernieuwingen. Wij besteden hieronder aandacht aan twee relatief nieuwe vormen van uitbesteding, namelijk *Banking-as-a-Service* en *cloud computing*.

Met *Banking-as-a-Service* bieden partijen bancaire infrastructuur aan voor banken en niet-banken. Op deze manier hoeven banken niet langer zelf alle systemen te onderhouden, maar gebruiken ze deze pakketten van derden. In Nederland zijn voorbeelden van banken die zo hun betaaldiensten uitbesteden. *Banking-as-a-Service* maakt het ook voor niet-banken mogelijk om bijvoorbeeld kredieten te verstrekken via zogeheten *white labeling*.[2] In dat geval maakt een niet-bank gebruik van zowel de bankvergunning van de *white label* verstrekker als van de onderliggende infrastructuur.

1 In onze definitie van een open bankensector is de waardeketen open en niet voorbehouden aan één entiteit, in dit geval de bank. Diverse partijen treden toe tot de keten, en de invoering van de nieuwe richtlijn *Payment Services Directive 2* (PSD2) zien we als één van de katalysatoren van de meer open bankensector. Onze definitie is daarmee ruimer dan de term *open banking* in het Verenigd Koninkrijk, die refereert aan de verplichting voor banken om, onder bepaalde voorwaarden, transactiedata met derde partijen te delen.
2 Van *white labeling* is sprake als een bedrijf een product of dienst merkloos verkoopt aan een ander bedrijf die dat vervolgens in de markt zet onder zijn eigen merknaam.

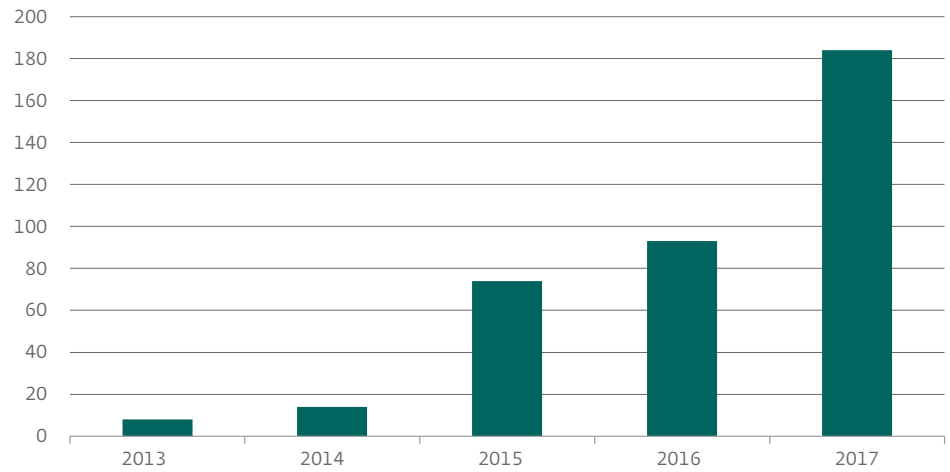
Figuur 1 Openheid in de waardeketen voor kredietverlening (gestileerd)



Een andere in belang toenemende vorm van uitbesteding is *cloud computing* diensten. Het aantal bij DNB gemelde *cloud computing* uitbestedingen is in de afgelopen vier jaar toegenomen tot ruim 180 in 2017 (zie figuur 2).[3] *Cloud computing* biedt de mogelijkheid om rekenkracht of verwerkingscapaciteit relatief eenvoudig en snel aan te passen. Hierdoor hoeven banken minder server- en computercapaciteit in eigen huis en in beheer te hebben. Banken kunnen verschillende IT-diensten verplaatsen naar de cloud, van de ondersteunende infrastructuur, zoals servers en opslagcapaciteit (*Infrastructure-as-a-Service*) tot softwareapplicaties, zoals email (*Software-as-a-Service*). Al deze gevallen worden gezien als een uitbesteding. De verwachting is dat banken in de nabije toekomst meer kerntaken, zoals consumentenbetalingen en *credit scoring* in de cloud zullen uitvoeren.[4]

Figuur 2 Aantal cloud uitbestedingen neemt snel toe

Aantal gemelde cloud uitbestedingen door banken in Nederland



Bron: DNB

3 De meldingen zijn afkomstig van 23 banken gevestigd in Nederland.
4 PWC (2016), "Financial Services Technology 2020 and Beyond: Embracing Disruption."

2.3 Openheid via samenwerkingen

Door samenwerkingsverbanden profiteren banken en nieuwe (fintech) partijen van elkaars sterke punten. Banken zijn vooral geïnteresseerd in de technologische kennis van fintechs (zie box 1). Waar vijf jaar geleden niet of nauwelijks melding werd gemaakt van partnerships met (fintech)partijen, rapporteren de Nederlandse drie grootbanken inmiddels meer dan 250 samenwerkingen. Ruim 90% van de Europese banken werkt samen met fintechs.[5] Voor de fintechs zijn contracten met banken aantrekkelijk vanwege toegang tot klantenbestand en -data, meer mogelijkheden tot het aantrekken van financiering, en ervaring met het voldoen aan wet- en regelgeving. Driekwart van de fintechs wereldwijd richt zich direct op samenwerken met gevestigde banken.[6] We onderscheiden twee soorten samenwerkingen. Ten eerste zijn er samenwerkingsvormen waarvoor banken zelf het initiatief nemen en tijd of budget voor reserveren, zoals deelnemingen in fintechs. Ten tweede onderscheiden we samenwerkingsvormen waarvoor de bank de randvoorwaarden creëert, maar het initiatief aan andere partijen laat. Een voorbeeld daarvan zijn *developer portals*. Dat zijn online omgevingen waar app- en softwareontwikkelaars nieuwe gebruikstoepassingen kunnen bouwen, gebruik makend van de bancaire infrastructuur.

Box 1 Artificiële intelligentie toepassingen in het bankwezen

Banken gebruiken in toenemende mate artificiële intelligentie (AI) toepassingen. Een open bankensector versterkt deze tendens, omdat banken in nauwe samenwerking met fintechs of via uitbesteding AI-toepassingen binnenhalen.[7] AI is een specialistisch vakgebied dat zich richt op de ontwikkeling van computersystemen die in staat zijn om taken uit te voeren die traditioneel menselijke intelligentie vereisen.[8] AI wordt reeds toegepast in direct contact met de klant. Denk aan de inzet van stemgestuurd bankieren en 24-uur beschikbare virtuele medewerkers (chatbots). Daarnaast worden met behulp van *machine learning* geavanceerde risicoanalyses uitgevoerd voor bijvoorbeeld geautomatiseerd beleggingsadvies. Ook wordt *machine learning* gebruikt om risicomodellen te leren patronen te ontdekken in grote hoeveelheden data. Dat 'leren' kan op twee verschillende manieren: (deels) onder menselijk toezicht en zonder menselijk toezicht.[9] In beide gevallen dienen besluiten onder verantwoordelijkheid van personen binnen de bank tot stand te komen, traceerbaar en uitlegbaar te zijn (zie hoofdstuk 5).

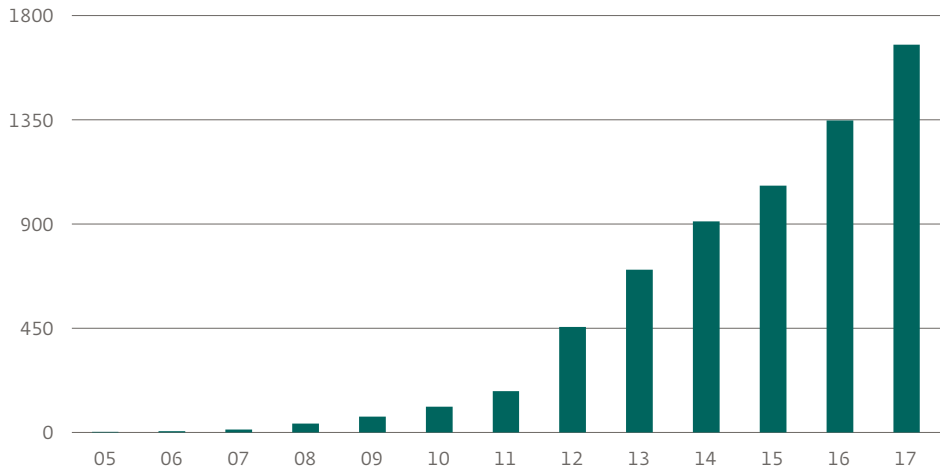
5 EBA (2018), "Report on the impact of fintech on incumbent credit institution's business models".
6 Capgemini (2017), "The World Fintech Report 2017".
7 Bafin (2018), "*Big data meets artificial intelligence. Challenges and implications for the supervision of and regulation of financial services*".
8 FSB (2017), "*Artificial intelligence and machine learning in financial services: Market developments and financial stability implications*".
9 In geval van onder toezicht leren leert een model met wat voor uitkomsten het moet komen aan de hand van data van een gelabelde dataset. Een gelabelde dataset houdt in dat alle gegevens een label hebben en dus bij een bepaalde categorie horen. De uitkomsten zijn van tevoren door iemand vastgesteld. In geval van leren zonder toezicht wordt het aan het model overgelaten om zelf de data te ontdekken en te ontleden. Het model trekt conclusies op basis van een niet gelabelde dataset. De uitkomsten zijn dus niet van tevoren bekend. Deels onder toezicht leren is een combinatie van de voorgaande twee technieken.

Banken werken via deelnemingen en andere investeringscontracten samen met fintechbedrijven. Ze maken uiteenlopende afspraken over risicodeling en verantwoordelijkheid. Banken kunnen joint-ventures opzetten met een derde partij en maken dan een vooraf vastgestelde verdeling van aansprakelijkheid en risico/winstdeling. Ook nemen banken deel in fintechbedrijven via hun *venture capital* fondsen. In Nederland hebben de drie grootbanken in totaal circa EUR 420 miljoen hiervoor beschikbaar. Met de investeringen uit deze fondsen wordt beoogd om kennis te vergaren die ingezet kan worden voor het eigen bedrijf. Maar er zijn ook lossere contractuele verbanden. Zo werkt een aantal internationale banken samen aan grensoverschrijdende betalingssystemen op basis van blockchain-technologie.

Banken faciliteren via *developers portals* ook de samenwerking met fintechbedrijven door zich 'technisch' open te stellen. Via *application programming interfaces* (API's) stellen ze hun infrastructuur open. Een API is een contactpunt dat computerapplicaties in staat stelt om met elkaar te communiceren en informatie (data) uit te wisselen over een netwerk. Door API's extern open te stellen, geeft een bank een derde partij gecontroleerd toegang tot (een deel van) haar infrastructuur en data.[10] Intern gebruiken banken al langer API's om IT-systemen met elkaar te laten communiceren. Het aantal publiek beschikbaar gestelde API's door banken is naar schatting de afgelopen jaren sterk gegroeid (zie figuur 3). Diverse Europese banken hebben *developer portals* om nieuwe toepassingen voor bancaire diensten te ontwerpen, zoals het invoegen van betaalopties in boekhoudsoftware voor ondernemers.

Figuur 3 API's steeds vaker toegepast in de financiële sector

Aantal openbare API's financiële sector wereldwijd



Bron: Accenture

10 Dit is anders bij *screen scraping*, waarbij een derde partij toegang kan krijgen tot de bankrekening van de klant met de inloggegevens van de klant.

2.4 Openheid via klantcontact

De bankensector wordt meer open doordat banken verplicht worden betaaldata te delen met derde partijen als de klant daar toestemming toe geeft. Dat volgt uit de nieuwe *Payment Services Directive 2* (PSD2) die in 2019 in werking treedt. Consumenten kunnen betalingen initiëren of hun rekeninggegevens inzien zonder direct contact met hun bank. Nieuwe partijen zoals rekeninginformatiedienst- en betaalinitiatiedienstverleners verzorgen dan de klantinteractie. [11] DNB heeft laten onderzoeken in hoeverre consumenten ook bereid zijn om hun betaaldata te delen met derde partijen (zie box 2).

Een aantal banken zet daarnaast zelf stappen om het klantcontact in de toekomst via een platform voor financiële dienstverlening te organiseren. Het aangaan van samenwerkingsverbanden met verschillende partijen is een eerste stap om complementaire diensten en producten via een platform te distribueren. Er zijn uiteenlopende definities van een platform.[12] Kenmerkend is dat het vragers en aanbieders van producten en diensten bij elkaar brengt en daarmee transactiekosten voor deelnemers verlaagt. Naast schaalvoordelen kent een platform netwerkeffecten, dat wil zeggen dat naarmate het aantal gebruikers op een platform toeneemt ook de toegevoegde waarde voor een individuele gebruiker toeneemt. Tot slot is kenmerkend dat een distributiegericht platform via data-analyse strategisch inspeelt op individuele wensen van gebruikers. Een aantal Europese banken heeft de ambitie uitgesproken om zelf uit te groeien tot een financieel platform waarop ook diensten van derden worden aangeboden, inclusief die van concurrenten.

Banken kunnen de rol aannemen van leverancier aan een platform of platformregisseur met verschillende gevolgen voor het klantcontact. Als leverancier distribueren banken hun producten en diensten via platformen van andere financiële instellingen of in de toekomst mogelijk via bigtechs. Een platform is voor banken in zo'n geval een extra distributiekanaal. Een zogenoemde platformregisseur beheert daartegen zijn eigen platform en onderhoudt daarmee ook de klantrelatie. Een platformregisseur zorgt er niet alleen voor dat transacties op het online platform gemakkelijk plaatsvinden, maar draagt ook zorg voor vertrouwen tussen vragers en aanbieders door onder meer de kwaliteit van de aangeboden producten te borgen.

Een van de kerntaken van een platformregisseur is daarom *due diligence* en management van de leveranciers, die actief zijn op zijn platform.[13] Een belangrijke vraag voor banken is of ze zelf platforms beheren of dat bigtechs deze rol innemen. In Azië zijn Alipay en Tencent, de twee Aziatische bigtechs, er in relatief korte tijd in geslaagd om 93% van de markt voor mobiele betalingen over te nemen.[14] Westerse bigtechs als Amazon en Facebook bieden recent ook betaalmogelijkheden aan op hun platformen, en zetten, vaak in samenwerking met banken, de eerste stappen richting andere bancaire activiteiten.

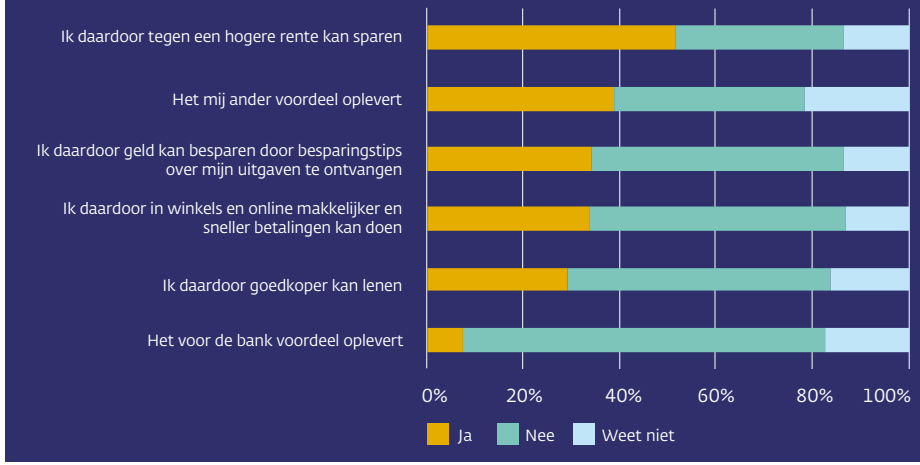
11 Op voorwaarde dat deze aanbieders onder toezicht staan van DNB.
12 We focussen hier op distributiegerichte platforms, dat wil zeggen platforms gericht op het klantcontact (aan de voorkant van de waardeketen). Er zijn ook productiegerichte platforms, dat zijn bijvoorbeeld de open API-platforms van banken waarop nieuwe producten worden ontwikkeld in het midden van de waardeketen (zie ook voorgaande paragraaf).
13 In de praktijk kan een bank die een platform beheert kan zelf ook zijn producten op een ander platform aanbieden.
14 Financial Times (2018), "*Tencent and Alipay set to lose $1bn in revenu from payment rules*". 15 juli 2018. Vanuit het betalingsverkeer hebben deze twee Aziatische bigtechs hun platformen gestaag uitgebreid met andere bancaire diensten, zoals kredietverlening en vermogensbeheer.

Box 2 Hoe bereid zijn Nederlandse consumenten om hun data te delen?

Het is niet zeker of rekeninghouders na invoering van PSD2 bereid zullen zijn om hun betaaldata te delen. DNB heeft middels een enquête in samenwerking met CenterData onderzocht hoe bereid consumenten zijn om hun betaaldata te delen en welke overwegingen hierbij een rol spelen. Circa 65% van de huishoudens zegt eerder aan hun bank toestemming te geven om hun betaaldata te gebruiken dan aan technologiebedrijven. De bereidheid blijkt verder af te hangen van de voordelen die huishoudens daarvoor terug krijgen (zie figuur 4). De animo om data te delen blijkt het sterkst als rekeninghouders een hogere rentevergoeding krijgen op hun spaargeld (52%). Dit percentage neemt toe naarmate rekeninghouders jonger zijn.

Figuur 4 Consument wil voordelen zien van gebruik betaalgegevens

Ik stem in met het gebruik van mijn betaalgegevens door mijn bank als het doel van het gebruik is dat...



3 Gevolgen voor instellingen

Een open bankensector heeft gevolgen voor partijen in de sector. In dit hoofdstuk bespreken we hoe de ontvlechting van waardeketens de operationele bedrijfsvoering, de beheersing van integriteitsrisico's, en tot slot verdienmodellen raakt.

3.1 Gevolgen voor operationele risico's

Een open bankensector biedt kansen voor het verbeteren van de operationele bedrijfsvoering. De kwaliteit en (kosten)efficiëntie van de bedrijfsvoering neemt toe als gewerkt wordt met gespecialiseerde technologiebedrijven die bepaalde taken beter kunnen uitvoeren tegen lagere kosten, zoals cyberveiligheid. Tegelijkertijd biedt het werken met derden banken de mogelijkheid om zich te concentreren op hun kerntaken. Tot slot leidt bijvoorbeeld het gebruik van clouddiensten tot meer operationele flexibiliteit.

Daar staat tegenover dat het type operationeel risico verandert omdat risico's verschuiven van interne risico's naar leveranciersrisico en regierisico.[15] Als de waardeketen een aaneenschakeling van afzonderlijke partijen wordt, is het lastiger voor banken om inzicht te hebben in hoe verantwoordelijkheden tussen partijen zijn belegd en of de kwaliteit van risicobeheersing van de betrokken partijen afdoende is. Risicobeheersing wordt gecompliceerder naarmate kernprocessen door meerdere derde partijen worden uitgevoerd, of wanneer dienstverleners aan banken zelf ook bedrijfsonderdelen uitbesteden aan derde partijen. Deze zogeheten onderuitbestedingen leiden tot langere en complexere ketens en bemoeilijken daarmee de operationele risicobeheersing. Het is daarom voor instellingen van belang dat dit in hun risicomanagement wordt geadresseerd, zoals we in hoofdstuk 5 nader zullen bespreken. In een aantal landen staan derde partijen onder direct financieel toezicht (zie box 3).

Het type operationeel risico verandert ook door de inzet van complexe technologieën. De kennisasymmetrie met derde partijen neemt toe naarmate technologische kennis meer specialistisch wordt. Technieken als *near field communication, biometrics, cloud computing* of *machine learning* zijn typische IT-vakgebieden, waarvan de toepassingsmogelijkheden in het bankbedrijf toenemen en die specialistische kennis vergen om deze op een adequate manier in te zetten en te beoordelen. Als de kennisasymmetrie toeneemt, zijn extra inspanningen noodzakelijk om voldoende 'in control' te blijven en voldoende kennis te hebben van de onderliggende techniek. Risico's die gepaard gaan met het toepassen van dergelijke technieken dienen ook geadresseerd te worden in het operationele beheersingsraamwerk van banken.

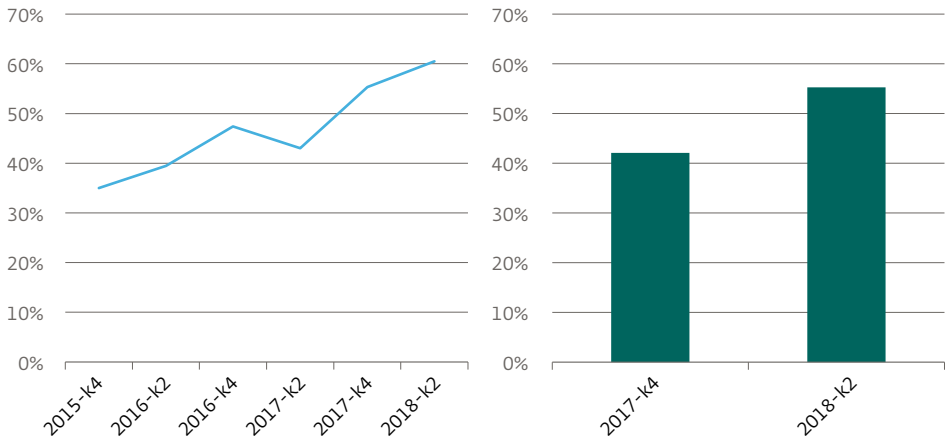
Tot slot neemt het relatieve belang van operationeel risico toe door het intensievere gebruik van data en verwevenheid tussen partijen via het internet. In een open bankensector hebben derde partijen toegang tot (gevoelige) data van banken, wat vereist dat banken voldoende inzicht hebben in welke data ze delen en of

15 Leveranciersrisico's hebben betrekking op de risico's die ontstaan vanuit de partij waaraan wordt uitbesteed. Dat kunnen bijvoorbeeld leveringsproblemen, dataschending of zelfs een faillissement zijn. Operationele risico's zijn volgens het BCBS alle risico's op verliezen door menselijk handelen, inadequate interne processen of systemen, of risico's door externe gebeurtenissen. Zie: BCBS (2011), "*Principles for the sound management of operational risk*".

databeveiliging bij derde partijen op orde is. De wettelijke eisen rondom databenutting zijn aangescherpt en in Nederland opgenomen in de Algemene Verordening Gegevensbescherming. Op grond van deze wet kunnen bij schendingen boetes worden geheven – tot 4% van de concernomzet – die in potentie de solvabiliteit van een bank kunnen raken. Dataveiligheid is daarmee zowel direct (via operationeel risico) als indirect (via financiële sancties) relevant voor prudentieel toezicht. Op het gebied van dataveiligheid en cyberrisico hebben banken te maken met meerdere toezichthouders.[16] Nederlandse en Europese banken herkennen zelf ook het toenemende belang van operationeel risico en de rol van dataveiligheid hierin (zie figuur 5).

Figuur 5 Banken zien toenemend operationeel risico en belang van dataveiligheid

Aandeel Europese banken dat operationeel risico ziet toenemen (linker paneel) en aandeel dat cyberrisico en dataveiligheid als belangrijke drijfveer hiervan ziet (rechterpaneel)



Bron: DNB, EBA Risk Assessment Survey

16 Onder meer de Autoriteit Persoonsgegevens, het Agentschap Telecom, de Autoriteit Financiële Markten, de Autoriteit Consument en Markt en DNB.

3.1 Gevolgen voor operationele risico's
3.2 Gevolgen voor integriteitsrisico's
3.3 Gevolgen voor verdienmodellen

Box 3 Toezicht op derde partijen – de reikwijdte van toezicht

In een aantal jurisdicties hebben financieel toezichthouders de mogelijkheid om direct toezicht te houden op derde partijen. In de Verenigde Staten kunnen federale toezichthouders vanuit hun wettelijke bevoegdheid inspecties uit voeren bij derde partijen.[17] Toezichthouders hebben op basis hiervan een specifiek toezichtraamwerk ontwikkeld voor *technology service providers* (TSPs), waarbinnen ze gezamenlijk toezicht houden op zowel systeemrelevante als regionale TSPs. Deze inspecties concentreren zich vooral op IT- en operationele risico's.

Luxemburg kent een vergunningsplicht voor derde partijen die specifieke diensten leveren aan financiële instellingen, onder de noemer *financial sector professionals* (PFS). Hieronder vallen belangrijke ondersteunende diensten zoals administratie- of IT-diensten, maar geen *cloud providers*. Bedrijven met een PFS-vergunning vallen onder direct toezicht van de nationale financiële toezichthouder CSSF. Overigens geldt ook hier –net als in de VS - dat financiële instellingen de uiteindelijke verantwoordelijkheid blijven dragen voor de risicobeheersing.

DNB houdt geen direct toezicht op derde partijen die werkzaamheden uitvoeren voor financiële instellingen. Wettelijk is vastgelegd dat de bank verantwoordelijkheid houdt over de uitbesteding. Bovendien moet in uitbestedingscontracten zijn vastgelegd dat de toezichthouder volledige toegang krijgt tot alle informatie en ook de mogelijkheid heeft om onderzoek ter plaatse uit te voeren (*'access, information and audit right'*). DNB is er scherp op dat dit *audit right* beschreven wordt in contracten, zodat inspecties bij derde partijen effectief kunnen plaatsvinden als er vanuit risico-oogpunt aanleiding toe is.

3.2 Gevolgen voor integriteitsrisico's

In een open bankensector kan de beheersing van integriteitsrisico's verbeteren. Banken kunnen bijvoorbeeld samenwerken op het gebied van *know your customer* onderzoek of het monitoren van verdachte transacties. Dit leidt mogelijk tot meer inzichten, waarmee financieel-economische criminaliteit kan worden aangepakt. In Nederland verkent een aantal banken of een private centrale eenheid voor *know your customer* onderzoek kan worden opgezet. Hoewel voor de opzet van een dergelijke samenwerking tal van praktische en juridische barrières geslecht dienen te worden, onder andere over het eigenaarschap van de eenheid, data en informatie, zou dit mogelijkerwijs tot effectievere en efficiëntere controles leiden. Een zelfde private samenwerking is denkbaar op het gebied van transactiemonitoring.

De effectiviteit van de poortwachters-rol van banken neemt mogelijk af als de keten uit meer schakels bestaat. *Customer due dilligence* kan zelf ook een aparte schakel worden via uitbesteding. In Nederland besteedt circa 20% van de banken een deel van het *customer due diligence* proces uit, zo blijkt uit een DNB-uitvraag. Dit betreft vooral het onderdeel klantacceptatie, omdat derde partijen het proces voor aanmelding (de zogeheten *onboarding*) van nieuwe rekeninghouders klantvriendelijker maken. Hierbij is het van belang dat de kwaliteit van de screening bij klantacceptatie geborgd blijft. De effectiviteit van de poortwachtersrol wordt daarnaast ook beproefd als banken via API's hun aanbod uitbreiden met diensten die de financieel-economische criminaliteit in de hand kunnen werken. Denk bijvoorbeeld aan cryptodiensten van derde partijen.[18] De inkomstenbron van crypto's is moeilijk

17 De federale toezichthouders zijn de Board of Governors of the Federal Reverse System (FRB), de Federal Deposit Insurance Corporation (FDIC) en de Office of the Comptroller of the Currency (OCC). Relevante wetteksten zijn te vinden in de Bank Service Company Act, 12 USC §1867(c).
18 Nieuwe online only banken in Europa bieden dergelijke diensten van derde partijen aan.

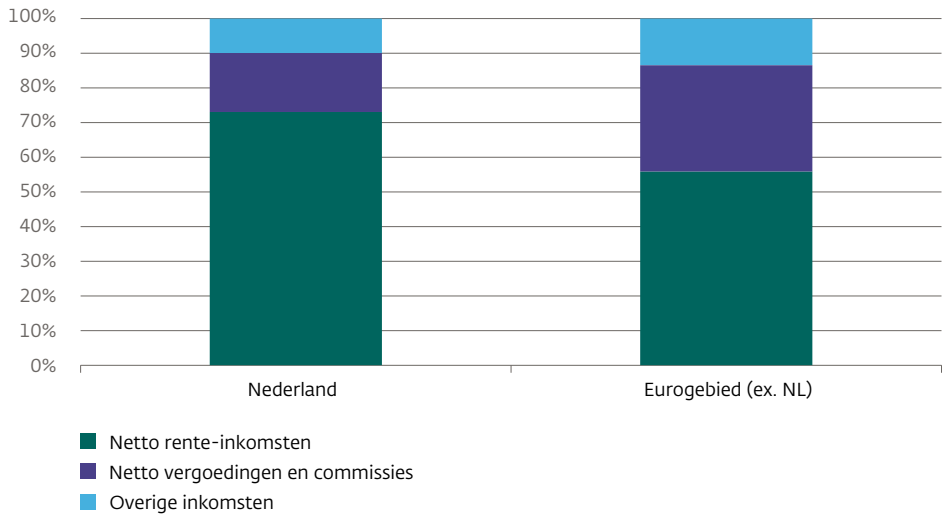
te achterhalen. Voor de integriteit van het financieel stelsel als geheel is het belangrijk dat voor aanbieders van bijvoorbeeld *cryptowallets* en crypto-omwisselplatforms dezelfde eisen gelden ten aanzien van het voorkomen van financieel-economische criminaliteit als voor financiële instellingen. Voor cryptodiensten zullen die eisen gaan gelden vanaf januari 2020.[19]

3.3 Gevolgen voor verdienmodellen

Een open bankensector biedt mogelijkheden voor diversificatie van het verdienmodel. Via het gebruik van API's kunnen banken nieuwe producten aanbieden zoals programma's om de identiteit van klanten digitaal vast te stellen, marktanalyses of factureringsdiensten. Ook zijn er – veelal nieuwe – banken die hun bancaire infrastructuur (*Banking-as-a-Service*) aanbieden. Kenmerkend voor deze productinnovaties is dat hierop transactie- , abonnements- of licentievergoedingen worden verdiend in plaats van rentemarges. Voor de Nederlandse banken zou dit betekenen dat de relatieve afhankelijkheid van de rente-inkomsten kan verminderen (zie figuur 6).

Een open bankensector kan winstmarges onder druk zetten als de openheid leidt tot meer concurrentie door toetreding van nieuwe spelers. Nieuwe partijen als *data aggregators* maken het makkelijker om te vergelijken tussen en over te stappen naar verschillende aanbieders, waardoor op termijn de rentegevoeligheid van deposito's kan toenemen. Uiteraard staat of valt dit effect met de mate waarin de consument openstaat voor dergelijke diensten van nieuwe spelers, en ook toestemming geeft aan derde partijen om data op te vragen.[20] Ook als deze *data aggregators* in de praktijk niet leiden tot meer overstappen, kunnen zij via meer transparantie over tariefstellingen zorgen voor prijsdruk.

Figuur 6 Samenstelling netto operationeel inkomen banken



Bron: DNB, ECB (2017)

19 Dit wordt geregeld in de 5e Anti-witwasrichtlijn waar lidstaten uiterlijk 10 januari 2020 aan moeten voldoen.
20 Uit een eerder onderzoek van (2014) blijkt bijvoorbeeld dat 73% van de Nederlanders boven de 18 jaar nog nooit is overgestapt van bank. Zie: ACM (2014), "Barrières voor toetreding tot de Nederlandse bancaire retailsector".

Ter illustratie: als Nederlandse banken als gevolg van grotere prijstransparantie 25 basispunten meer zouden moeten betalen over deposito's stijgen de rente-uitgaven volgens berekeningen ceteris paribus met 830 miljoen, een bedrag wat gelijk staat aan 5,5% van de totale winst voor belasting.[21]

Op de langere termijn kunnen winstmarges worden gedrukt als banken het klantencontact verliezen, en daarmee de mogelijkheden om andere producten te verkopen aan diezelfde klant (cross-selling).[22] De open bankensector kan de relatie tussen de klant en de bank veranderen. Waar rekeninghouders voor hun betalingsverkeer traditioneel voor elke transactie in contact stonden met hun bank, zijn ze dat door internetapplicaties als Paypal of mobiele betalingen steeds minder.

Door de komst van *wallets* in mobiele telefoons verdwijnt de bank op het oog naar de achtergrond. Daarnaast komen mogelijk betaalinitiatiediensten in de markt die eveneens het directe contact tussen bank en klant overnemen. Tot slot bepaalt de rol van de bank in de keten of een bank het primaire klantcontact onderhoudt en heeft daarmee gevolgen voor het verdienmodel van de bank. Deze rol hangt onder meer samen met de mate en snelheid van platformisering van de sector.

21 25 basispunten komt overeen met het verschil tussen de laagste en hoogste aanbieder in de spaarmarkt.
22 PwC (2016) Trendrapport over FinTech en nieuwe technologieën "De bancaire sector 'ouderwets' innovatief." Uit PwC-analyses blijkt dat mogelijkheden voor *cross-selling* circa drie keer hoger zijn bij klanten met een betaalrekening dan bij klanten zonder een betaalrekening. Spaarrekeningen zijn ook een voorbeeld van de *cross-selling* producten.

4 Gevolgen voor het financieel systeem

Een open bankensector heeft naast gevolgen voor individuele instellingen ook gevolgen voor de stabiliteit van het financieel systeem als geheel. In dit hoofdstuk gaan we eerst in op de kansen voor het financieel systeem, om vervolgens te bespreken welke risico's de ontvlechting van de waardeketen met zich meebrengt.

4.1 Kansen voor het financieel systeem

De toetreding van nieuwe partijen tot de waardeketen draagt bij aan hogere efficiëntie van de financiële dienstverlening en diversiteit in de sector. In de eerste plaats zorgt een open bankensector voor meer concurrentie en prijstransparantie. Daar komt bij dat nieuwe partijen dankzij hun digitale bedrijfsmodel en het gebruik van nieuwe technologie hun diensten efficiënter kunnen aanbieden. De nieuwkomers stimuleren gevestigde instellingen om te investeren in de modernisering van hun dienstverlening. Dit kan leiden tot lagere marges op financiële producten, die zich vervolgens vertalen in lagere prijzen voor de consument. In de tweede plaats vermindert de afhankelijkheid van een kleine groep instellingen, als meerdere partijen dezelfde diensten kunnen aanbieden. De kwetsbaarheid van het financiële systeem als geheel neemt daarmee af.

Een open bankensector heeft gevolgen voor de afwikkelbaarheid van banken. Als ketenonderdelen via *plug-and-play*-systemen eenvoudiger los- en aan te koppelen zijn, kan in resolutie makkelijker de kern van een bank worden voortgezet, en hoeft niet de gehele bank in resolutie te worden genomen. Daar staat tegenover dat de toenemende complexiteit van samenwerkingen en uitbestedingen het mogelijk lastiger maakt om te overzien welke partijen verantwoordelijk zijn voor welke activiteiten. Het is daarbij belangrijk dat banken in de *service-level agreements* met derde partijen geen voorwaarden hebben staan die voortzetting in resolutie kan belemmeren.

4.2 Risico's voor het financieel systeem

Sector- en grensoverschrijdende verwevenheid tussen partijen nemen toe in een open bankensector. De IT-verbindingen tussen banken onderling en tussen banken en tech-bedrijven nemen mogelijk toe, waardoor het risico op besmetting bij een operationele storing groter wordt. Op termijn kan de sector-overschrijdende verwevenheid verder toenemen, omdat een aantal gevestigde banken toewerkt naar activiteiten die buiten de eigen branche liggen. In de sector wordt hieraan gerefereerd als *beyond banking*. Zo kunnen banken makelaarsdiensten, aanbieden in combinatie met hun eigen financiële producten. Deze vermenging met andere sectoren biedt kansen voor een diverser verdienmodel, maar kan ook reputationele risico's aan boord halen voor individuele instellingen. Tot slot maakt de combinatie van een digitaal bedrijfsmodel en een Europees paspoort het relatief gemakkelijk om bancaire diensten in meerdere landen aan te bieden. Een betaalinstelling kan bijvoorbeeld dankzij een vergunning van één Europese autoriteit ook andere landen in Europa bedienen zonder daar actief onder toezicht te staan.

4.1 Kansen voor het financieel systeem
4.2 Risico's voor het financieel systeem

Risico's kunnen verschuiven naar (nieuwe) partijen die zich niet aan dezelfde of vergelijkbare regelgeving hoeven te houden als bestaande financiële instellingen. Partijen zonder oorsprong in de financiële sector (en bekendheid met regulering ervan) treden toe tot de keten.
Zij beheersen bepaalde risico's mogelijk minder goed omdat bijvoorbeeld gebruikte modellen niet een volledige kredietcyclus hebben doorlopen.
Denk aan de kredietrisicomodellen met zelflerende algoritmes, die veelal worden gebruikt door *online market place lenders*, waarvan het nog moet blijken of hun voorspelkracht in een recessie adequaat is[23]. Een ander voorbeeld zit op het terrein van cyberrisico's. Europese toezichthouders werken samen met banken aan de cyberweerbaarheid van de financiële sector door programma's van *red teaming* (ethisch hacken).

De effectiviteit van deze toezichtaanpak vermindert als banken hun IT verplaatsen naar partijen die hier niet aan mee werken, waardoor inzichten in cyberrisico's mogelijk onvolledig zijn of achterblijven.

Bij (onder)uitbestedingen kunnen zich concentratierisico's opbouwen als banken gebruik maken van dezelfde dienstverleners. Een individuele bank heeft geen inzicht in mogelijke concentratierisico's op sectorniveau en maakt een afweging voor een dienstverlener op basis van de voordelen die dat met zich meebrengt voor haar eigen bedrijfsvoering. Daarmee kunnen dergelijke dienstverleners een *single point of failure* veroorzaken, wat kan leiden tot uitval van cruciale dienstverlening – zoals betalingstransacties – op systeemniveau.

Dit brengt niet alleen de bedrijfscontinuïteit van afzonderlijke instellingen in gevaar, maar kan ook het vertrouwen in de bankensector ondermijnen. De concentratie in de clouddienstensector neemt bijvoorbeeld toe, waarbij vier grote partijen 60% van de wereldwijde markt voor hun rekening nemen.[24] Onderuitbestedingen kunnen potentiële concentratierisico's verder versterken. Partijen aan wie banken uitbesteden kunnen immers op hun beurt weer gebruik maken van dezelfde dienstverleners. In de praktijk maken fintechs ook gebruik van internationale clouddienstverleners en datacenters.

4.1 Kansen voor het financieel systeem
4.2 Risico's voor het financieel systeem

23 Claessens, S., Frost, J., Turner, G. and Zhu, F. (2018) "Fintech credit markets around the world: size, drivers and policy issues", BIS Quarterly Review, September.
24 Synergy Research Group (2017), "Cloud Market Keeps Growing at Over 40%; Amazon Still Increases its Share," October. Dit betreft de volledige markt voor clouddiensten, niet enkel voor financiële instellingen.

5 Aandachtspunten en vervolgstappen

DNB vindt innovatie noodzakelijk voor een op langere termijn levensvatbare bancaire sector. Vernieuwing gaat echter ook gepaard met risico's. DNB wil tijdig en helder aan de bancaire sector laten weten wat de verwachtingen vanuit toezicht zijn. Het doel hiervan is om te zorgen voor goede randvoorwaarden voor innovatie en de impact van potentiële incidenten in een meer open bankensector te verminderen. Goed toezicht is geen statisch gegeven, maar vergt continu inspelen op veranderingen in de financiële sector. We zetten daarom graag de dialoog voort met marktpartijen om te zorgen dat toezicht niet onnodig vernieuwingen remt. Initiatieven zoals de InnovationHub en Maatwerk voor Innovatie kunnen hiervoor worden benut.

5.1 Aandachtspunten voor de sector

Banken die taken uitbesteden blijven verantwoordelijk voor het beheersen van risico's van deze taken en diensten. De Wet op het financieel toezicht (Wft) staat onder voorwaarden toe dat banken bepaalde werkzaamheden uitbesteden aan derde partijen. Dit houdt in dat een bank dient te beschikken over adequaat beleid, procedures en maatregelen voor het uitbesteden van werkzaamheden, en dat het uitbesteden van activiteiten nooit een belemmering mag vormen voor het toezicht van DNB.[25] Voor clouddiensten gelden de nieuwe richtlijnen die de *European Banking Authority* (EBA) in 2018 heeft opgesteld.[26]

DNB werkt momenteel in EBA-verband aan aanscherping van de uitbestedingsrichtlijnen en deze worden geïmplementeerd in het Europees gemeenschappelijke toezicht. In de kern komen de aanscherpingen erop neer dat instellingen geen 'lege huls' mogen worden. Verantwoordelijkheden van het bestuur kunnen nooit worden overgedragen aan andere partijen. Tevens beschrijven de richtlijnen een raamwerk voor het *due diligence proces* bij uitbestedingen. Dit moet eraan bijdragen dat instellingen in staat zijn om alle risico's te overzien en te beheersen, de kwaliteit en resultaten van het uitbestede werk voortdurend te toetsen. DNB zal conform deze richtlijnen toezien.

Ook als activiteiten door derden niet onder de letterlijke definitie van uitbestedingen vallen dienen banken een adequaat risicoraamwerk te gebruiken. Banken blijven verantwoordelijk voor een integere en beheerste bedrijfsvoering. Invulling daarvan betekent dat banken de *due dilligence* van derde partijen goed managen en doorlopend inzicht hebben in de risico's waaraan zij worden blootgesteld door de samenwerking met derde partijen. Beheersingsmaatregelen dienen daarbij proportioneel te zijn ten opzichte van de risico's die een bank loopt, ook als activiteiten volgens de bank niet onder de definitie van uitbesteding vallen.[27]

25 Zie artikel 3.18 van de Wft De Europese richtlijnen op het gebied van uitbestedingen stammen uit 2006, en worden momenteel door de *European Bank Authority* (EBA) herzien. Deze richtlijnen stellen nadere eisen aan het beheersingsraamwerk en *governance* van banken ten aanzien van uitbestedingen, en moeten leiden tot een meer geharmoniseerd raamwerk op Europees niveau.

26 EBA (2017), "Recommendations on outsourcing to cloud computing service providers". De richtlijn is per 1 juli 2018 ingevoerd.

27 In de toezichtpraktijk zijn voorbeelden van discussies tussen instellingen en toezichthouders over de vraag of sprake is van een formele uitbesteding of inkoop van een gestandaardiseerde dienst. In de concept uitbestedingsrichtlijnen van de EBA wordt verduidelijkt wat wordt verstaan onder een uitbesteding door te verwijzen naar "kritieke en belangrijke processen" die door derden worden gedaan. Ondanks deze nadere toelichting valt niet uit te sluiten dat ook in de toekomst interpretatieverschillen ontstaan. DNB wijst ook daarom op het generieke belang van risicobeheersing als wordt gewerkt met derde partijen.

Bij alle samenwerkingen vindt DNB het belangrijk dat banken in hun operationeel beheersingsraamwerk risico's van innovatieve technieken adequaat adresseren. Een concreet voorbeeld is het gebruik van artificiële intelligentie toepassingen, zoals *machine learning*. Het gebruik van AI – veelal via derde partijen – mag niet leiden tot een verschuiving van de verantwoordelijkheid van personen naar machines. Op hoofdlijnen verwacht DNB daarom dat de verantwoordelijkheid voor besluiten volgend uit AI duidelijk binnen de organisatie zijn belegd, en net als andere besluiten traceerbaar en uitlegbaar zijn.[28] Tot slot dienen organisaties zich bewust te zijn van ethische kwesties rondom AI-toepassingen, zoals het risico op vooringenomenheid door bijvoorbeeld vertekende informatie (*biases*).

Omdat AI toepassingen van meerwaarde kunnen zijn voor banken en tegelijkertijd nieuwe vragen oproepen bij instellingen en het toezicht, zal DNB komende periode nader onderzoek verrichten naar dit specifieke thema.

In het toezicht is groeiende aandacht voor de operationele weerbaarheid van instellingen. Dit betekent dat DNB er op toeziet dat banken plannen hebben om hun operatie weer snel opgestart te krijgen in geval van uitval of verstoring bij derden. DNB verwacht bijvoorbeeld dat er gewisseld kan worden van dienstverleners als continuïteit van dienstverlening wordt vereist. Op dit moment is de eis voor operationele weerbaarheid uitgangspunt voor het toezicht op kernbetaalinfrastructuren, maar de reikwijdte hiervan breidt zich uit naar andere bancaire activiteiten. [29]

Banken dienen aandacht te besteden aan de houdbaarheid van hun verdienmodellen op de lange termijn. Een relevante ontwikkeling hierbij is de mogelijke platformisering van de sector en de daarbij behorende vragen of banken zelf de klantrelaties willen en kunnen vasthouden. Het is aan de banken zelf om een strategische keus te maken. Daarbij is niet alleen de strategische ambitie relevant, maar ook het verandervermogen van de organisatie om deze ambitie ook daadwerkelijk tot uitvoering te brengen. Als banken de rol van regisseur nastreven, impliceert dit een ingrijpende omvorming van het bedrijfsmodel. Daarbij past capaciteitsonwikkeling op het gebied van bijvoorbeeld data-analyse en de selectie van derde partijen. Voor een bank in de rol van leverancier is het platform vooral een distributiekanaal met minder mogelijkheden tot *cross-selling*.

Daarom is het in deze rol des te belangrijker om de *cost-to-income* ratio beheersbaar te houden en de kostenbasis zoveel mogelijk te flexibiliseren.

5.2 Vervolgstappen voor het toezicht

Het is van belang dat toezichthouders beter overzicht krijgen van mogelijke concentratierisico's bij uitbestedingen. Dit is nodig om tijdig aanvullende eisen te kunnen stellen aan banken indien door een *single point of failure* de continuïteit van dienstverlening in gevaar komt. Banken hebben daarom sinds dit jaar de plicht om materiële cloud uitbestedingen te melden[30], en vanaf medio 2019 moeten ze ook overige uitbestedingen registreren.[31] DNB zal systematisch in kaart brengen of concentratierisico's optreden.

28 De nadere invulling van traceerbaarheid en uitlegbaarheid is onderwerp van vervolgonderzoek. Hierbij zal ook aansluiting worden gezocht met bijvoorbeeld de FSB en het SSM. Bij traceerbaarheid ligt de nadruk op welke stappen in het proces zijn ondernomen voor een besluit. Bij uitlegbaarheid ligt de nadruk op hoe tot een besluit is gekomen.
29 De werkgroep operational resilience van Het Bazelse comité voor Bankentoezicht (BCBS) is voornemens om in 2019 onderzoek te doen naar de wenselijkheid van basisprincipes voor operationele weerbaarheid.
30 EBA (2017), "Recommendations on outsourcing to cloud computing service providers".
31 EBA (2018), "Consultation paper on draft guidelines on outsourcing arrangements".

5.1 Aandachtspunten voor de sector
5.2 Vervolgstappen voor het toezicht

Hierbij zijn ook de onderuitbestedingen in beeld.[32] Inzichten in concentraties zullen indien nodig vanuit risico-oogpunt met instellingen worden gedeeld.

Daarnaast geven de potentiële concentratierisico's bij bijvoorbeeld *cloud service providers* aanleiding tot een onderzoek of bepaalde dienstverleners als *too big to fail* moeten worden gezien. Dit vraagstuk kan niet nationaal worden opgelost, maar vraagt om een internationaal gecoördineerde aanpak. Ten eerste omdat het gaat om grensoverschrijdende dienstverlening en potentiële concentraties een mondiaal risico zijn. Ten tweede omdat het noodzakelijk is om data op internationaal niveau te verkrijgen. Op termijn kan – op internationaal niveau – worden overwogen om de allergrootste dienstverleners, gemeten naar concentratiegraad, onder een vorm van toezicht te plaatsen.
De Amerikaanse toezichtpraktijk van derde partijen (zoals beschreven in de box 3) biedt in dat verband interessante aanknopingspunten en is mogelijk ook op Europees of internationaal niveau wenselijk.[33]

DNB gaat verdiepend beleids-onderzoek doen naar verdienmodellen van en databenutting door banken. Het onderzoek naar verdienmodellen richt zich op de middellange termijn van drie tot vijf jaar. Doel is om enerzijds een bijdrage te leveren aan het maatschappelijke debat over de rol van banken. Anderzijds dient dit ter ondersteuning van het (Europese) toezicht op bedrijfsmodellen van banken.

Een open bankensector vraagt op termijn wellicht om ruimere (wettelijke) mogelijkheden tot samenwerking tussen toezichthouders met verschillende mandaten. In een open bankensector is op bepaalde terreinen, zoals IT en het gebruik van data door banken en derde partijen, coördinatie nodig tussen verschillende (niet-)financiële toezichthouders.

Op de eerder genoemde terreinen IT en data zijn ten minste vijf toezichthouders bevoegd: het Agentschap Telecom ziet toe op de Wet beveiliging netwerk- en informatiesystemen, de Autoriteit Persoonsgegevens op het adequaat verwerken van persoonsgegevens, de AFM ziet erop toe dat de regels rondom zorgplicht worden nageleefd, de ACM ziet erop toe dat derde partijen toegang krijgen tot de financiële sector en DNB bewaakt de financiële soliditeit en integriteit van een instelling.

Naarmate er meer raakvlakken ontstaan is het van belang te zorgen voor een goede afbakening van elkaars verantwoordelijkheden. Daarnaast kan de effectiviteit van toezicht worden vergroot door kennisuitwisseling tussen toezichthouders te faciliteren. Waar nodig en wenselijk moet in samenspraak met collega toezichthouders worden bezien of uitbreiding van bestaande of aanvullende wettelijke bepalingen en samenwerkingsconvenanten nodig zijn.

32 Partijen aan wie kritische processen zijn uitbesteed moeten aan de bank melden wanneer zij op hun beurt ook weer activiteiten door derden laten uitvoeren. Als deze activiteit materieel genoeg is dient ook de toezichthouder hiervan op de hoogte worden gebracht.
33 Concentratierisico's kunnen ook via andere routes dan via het financieel toezicht worden gemitigeerd. Zo stimuleert de Europese Commissie clouddienstverleners om te komen tot gedragscodes en afspraken waardoor gebruikers gemakkelijker kunnen wisselen tussen dienstverleners.

Deze studie is mede tot stand gekomen dankzij interviews bij banken, fintechs, academici en collega toezichthouders. Wij danken alle gesprekspartners voor hun betrokkenheid en openhartigheid. Ria Roerink, Danijela Piljic en Kasper Goosen.

5.1 Aandachtspunten voor de sector
5.2 Vervolgstappen voor het toezicht