Alle banken

De Nederlandsche Bank N.V.
Resolutie

Postbus 98
1000 AB Amsterdam
+31 20 524 91 11
www.dnb.nl

Handelsregister 3300 3396

Onderwerp
Evaluatie audits Beleidsregel Individueel Klantbeeld

Datum
30 March 2021

Uw kenmerk

Ons kenmerk
T052-85402729-544

Behandeld door
Kooy, H.M. (Hans)

Telefoonnummer:

Mailadres:

Bijlagen

De Beleidsregel Individueel Klantbeeld schrijft voor dat banken door de interne accountantsdienst (IAD) en de externe accountant moeten laten toetsen of aan de voorschriften uit de beleidsregel is voldaan (zie ook artikel 11 en 12 van de beleidsregel; hierna: IKB-audits). In NVB-verband is samen met een delegatie van banken en accountantskantoren een evaluatie gedaan van de IKB-audits. Deze brief geeft een toelichting op de aanpassingen die DNB naar aanleiding van deze evaluatie doorvoert. De aanpassingen gaan in vanaf de eerstvolgende verslagperiode, die start op 1 april 2021.

De volgende punten komen aan de orde:

a) verslagperiode voor de IKB-audits van de IAD en de externe accountant
b) auditstandaard voor de toetsing door de externe accountant
c) samenhang tussen de werkzaamheden van de IAD en de externe accountant
d) proportionaliteit
e) toepassen van carve-outs in verband met uitbesteding van processen en diensten
f) inzicht in maatregelen die bevindingen wegnemen en de voortgang daarop
g) samenhang met audits op KYC-processen van een bank
h) nadere guidance bij het generieke beheersingsraamwerk

a) Verslagperiode voor de IKB-audits blijft 1 april – 31 maart
In de beleidsregel staat dat de oordeelsvorming plaatsvindt over het verslagjaar. De periode van het verslagjaar is in 2019 in overleg met banken vastgesteld op 1 april – 31 maart. Tijdens de evaluatie is gesproken over deze periode. Enkele banken deden het verzoek om de auditperiode gelijk te stellen aan het kalenderjaar. Een alternatief dat is geopperd was om de auditperiode van 1 juli – 30 juni te laten lopen. Naar aanleiding van de discussie hierover heeft DNB de deelnemende banken gevraagd om hun voorkeur. Daaruit bleek dat de ruime meerderheid wil vasthouden aan de periode 1 april – 31 maart.

b) **De auditstandaard voor de assuranceverklaring van de externe accountant blijft voorlopig ISAE 3402**
In de beleidsregel is vastgelegd dat de opdracht aan een externe accountant moet zijn gebaseerd op ISAE 3402, waarbij niet alleen opzet en bestaan, maar ook de werking onderdeel van toetsing is (type 2). Tijdens de evaluatie is door de accountantskantoren en enkele banken geopperd om de auditstandaard te wijzigen in ISAE 3000. Het belangrijkste argument daarvoor is dat deze standaard meer ruimte geeft voor de externe accountant voor gegevensgerichte controle met betrekking tot datakwaliteit.

DNB heeft eerder, in overleg met externe accountants en banken, bewust gekozen voor de ISAE 3402 standaard, en daarmee een procesgerichte audit. Achtergrond is dat het de verantwoordelijkheid is van banken om de relevante processen en beheersingsmaatregelen aan te passen aan de hoge mate van nauwkeurigheid die van banken wordt gevraagd. De interne beheersing van banken moet dusdanig goed zijn, dat de kans op fouten verwaarloosbaar is (gerichtheid op nul fouten, zoals toegelicht in de beleidsregel). Dit vraagt veel van banken en dit vergt tijd, waarbij banken een groeipad doorlopen om eventuele gaten te dichten.

Tijdens de evaluatie is uitgebreid gesproken over het nut en de toegevoegde waarde van gegevensgerichte controle. DNB is van mening dat het risico bestaat dat dergelijke controles afleiden van de aanpassing van onderliggende processen en beheersingsmaatregelen door banken. Daarop zou in deze fase de focus moeten liggen. Overigens past gegevensgerichte controle prima binnen het beheersingsraamwerk van de bank zelf. We zien dat banken dat ook steeds meer toevoegen aan hun controleraamwerk. Een juiste werking van de gegevensgerichte controle als onderdeel van het controleraamwerk van banken kan vervolgens worden getoetst op opzet, bestaan en werking binnen de ISAE 3402 standaard.

DNB sluit niet uit dat in de toekomst opnieuw wordt gekeken naar de ISAE standaard voor de toetsing door de externe accountant. Vooralsnog wordt ISAE 3402 als standaard gehandhaafd.

Overigens is door enkele banken ook geopperd om te kijken naar andere standaarden, waaronder COS 4400N (Overeengekomen specifieke werkzaamheden). Deze zijn voor DNB niet acceptabel, omdat deze standaarden niet de door DNB gevraagde mate van betrouwbaarheid geven.

c) **IAD en externe accountant hebben een verschillende rol in het IKB-raamwerk**

De afgelopen jaren is diverse keren gesproken over de samenhang en rolverdeling van de IAD en externe accountant in het IKB-raamwerk. Banken geven aan dat op dit punt desondanks nog onduidelijkheden bestaan. Aandachtspunten zijn onder andere het voorkomen van overlap in werkzaamheden en het uitvoeren van audits bij buitenlandse bijkantoren. DNB onderschrijft dat overlap in werkzaamheden zoveel mogelijk moet worden voorkomen. Tegelijkertijd hebben de IAD en externe accountants een verschillende rol.

Uitgangspunt is dat DNB zekerheid krijgt van de externe accountant dat een bank de vereisten in de Beleidsregel Individueel Klantbeeld naleeft, dat wil zeggen de beheersingsmaatregelen voor de relevante processen met een hoge mate van nauwkeurigheid toepast. De externe accountant moet dit aantoonbaar kunnen vaststellen. Het werkprogramma van de externe accountant is daarop gericht. De IAD daarentegen is onderdeel van het beheersingsraamwerk van de bank. De werkzaamheden van de IAD zijn onderdeel van de three-lines-of-defence van de bank. Naar onze opvatting is er een wisselwerking tussen het werkprogramma van de externe accountant en de werking van de three-lines-of-defence. Naarmate de three-lines-of-defence beter functioneert, kan het werkprogramma van de externe accountant beperkter zijn. Verder toetst de externe accountant of de rol van de IAD wordt ingevuld conform de vereisten in artikel 11 van de Beleidsregel Individueel Klantbeeld. Hiervoor is vorig jaar een beheersingsdoelstelling toegevoegd aan het generieke Controle Raamwerk (9.1).

De huidige guidance roept op dit punt veel vragen op en schept verwarring. De

guidance luidt dat "*de bank op basis van haar risicoanalyse tot de conclusie kan komen dat beheersingsmaatregelen met betrekking tot reguliere processen niet aanvullend door de externe accountant behoeft te worden getoetst, mits voldaan wordt aan een aantal voorwaarden"*. In de praktijk blijkt dit niet te werken en kiezen banken in overleg met de externe accountant om alle processen en bijbehorende beheersingsmaatregelen in scope te nemen. Daarbij speelt mee dat DNB in de beleidsregel geen nadere eisen stelt aan de rapportage van de IAD (free format). Alleen een volledige toetsing door de externe accountant geeft de gevraagde zekerheid.

Conclusie is dat deze keuzemogelijkheid met ingang van het komende verslagjaar (startend op 1 april 2021) verdwijnt. De opdracht aan de externe accountant moet alle relevante processen en beheersingsmaatregelen afdekken.

Voorgaande neemt niet weg dat de rapportage van de IAD zeer waardevolle aanvullende inzichten geeft over de mate waarin de bank de IKB-vereisten naleeft. In de rapporten van IAD's van banken wordt veelal dieper ingegaan op de borging van beheersingsmaatregelen en problemen op het gebied van datakwaliteit. Wel zien wij verschillen in diepgang van de IAD-rapporten van banken. DNB verwacht voldoende detailniveau van het rapport dat DNB inzicht geeft in de verbeteringen die nog moeten worden gerealiseerd om aan de vereisten uit de IKB beleidsregel te kunnen voldoen.

d) **Proportionaliteit is gewaarborgd**
Met name kleinere banken vragen aandacht voor de proportionaliteit van de IKB-audits, in het bijzonder de ISAE 3402 opdracht. Tijdens de evaluatie is besproken dat proportionaliteit voldoende is gewaarborgd bij het toepassen van de ISAE 3402 audit. Ook van kleinere banken vraagt DNB assurance dat de vereisten in de beleidsregel worden nageleefd. Tegelijkertijd hangt de omvang van de werkzaamheden nauw samen met de omvang en complexiteit van de bank.

e) **Toepassen carve-out alleen onder voorwaarden**
Veel banken besteden processen uit aan externe dienstverleners. In de ISAE 3402 audits worden deze onderdelen vervolgens via een carve-out buiten scope van de opdracht geplaatst. Hierdoor krijgt DNB niet altijd de gevraagde assurance. Banken zijn verantwoordelijk voor de beheersing van alle relevante processen en systemen. Hoewel DNB voorkeur geeft aan het zoveel mogelijk vermijden van carve-outs, onderkennen wij dat het toepassen van een carve-out soms onvermijdelijk is. Met name grote IT-dienstverleners sluiten specifieke audits in hun contractuele voorwaarden veelal uit.

DNB accepteert het toepassen van een carve-out, mits wordt voldaan aan de volgende voorwaarden:
- de vereisten uit de Beleidsregel Individueel Klantbeeld worden aantoonbaar geborgd in de contractuele afspraken en de bijbehorende dienstverleningsniveaus
- de bank verkrijgt van haar externe dienstverleners een assurance rapport (gebaseerd op de ISAE 3402 standaard of op de SOC 1 of SOC 2 standaard) dat expliciet de beheersingsmaatregelen afdekt uit het Controle Raamwerk die de bank heeft uitbesteed aan de externe dienstverlener.
- de rapportageperiode van dat assurance rapport komt òf overeen met de assurance periode die de bank hanteert voor de ISAE 3402 rapportage om te voldoen aan de Beleidsregel Individueel Klantbeeld, òf de bank verkrijgt van de externe dienstverlener een bridge letter voor de periode waarover geen assurance is verkregen.

- de bank neemt monitorende beheersingsmaatregelen[1] die aantonen dat de uitbestede processen voldoen aan de vereisten uit de beleidsregel op in het beheersingsraamwerk voor de ISAE 3402 rapportage van de bank zelf.
- De accountant rapporteert bij haar testwerkzaamheden op deze monitorende beheersingsmaatregelen hoe er is voldaan aan de vereisten dat (a) de uitbestede beheersingsmaatregelen zijn afgedekt in de assurance rapportage van de externe dienstverlener, (b) de rapportageperiode van de externe dienstverlener ofwel gelijk is aan de assurance periode of dat er een bridge letter is ontvangen voor de periode waarover geen assurance is verkregen en (c) de beheersingsmaatregelen door de accountant van de externe dienstverlener als effectief zijn beoordeeld, of voor welke beheersingsmaatregelen de accountant van de externe dienstverlener(s) heeft vastgesteld dat deze niet effectief zijn geweest.

Bovenstaande borgt dat DNB zekerheid krijgt over alle relevante processen en systemen. Mocht het voor de bank niet mogelijk zijn om aan deze vereisten te voldoen dan dient met de DNB te worden afgestemd hoe in de specifieke situatie met deze vereisten dient te worden omgegaan.

f) **Verbeteren inzicht in maatregelen die bevindingen wegnemen en de voortgang daarop**
Naast het verstrekken van de mate van betrouwbaarheid via het ISAE 3402 rapport, zijn het rapport van de IAD en het ISAE 3402 rapport een belangrijk instrument om verbeteringen door te voeren. DNB verwacht daarom in deze rapporten een managementrespons, waarin per bevinding een toelichting wordt gegeven op de opvolging van de bevindingen van het voorgaande rapport, en het actieplan met tijdspaden op de nog openstaande en nieuw geconstateerde bevindingen.

De ISAE 3402 standaard biedt hiervoor de mogelijkheid via een aanvullende sectie V. Diverse banken gebruiken deze aanvullende sectie. DNB vraagt alle banken om deze sectie voortaan standaard op te nemen in het ISAE 3402 rapport. In deze sectie kan tevens worden ingegaan op verbeteringen die inmiddels na de verslagperiode zijn doorgevoerd.

g) **Samenhang met audits op KYC-processen benutten**
Banken vragen naar de samenhang tussen de beheersing van KYC-processen en de vereisten in de Beleidsregel Individueel Klantbeeld. Banken geven daarbij aan dat KYC erg breed is, waarvoor veelal aparte controleprogramma's zijn ingericht op grond van de vereisten in de Wwft. Deze eisen gaan verder dan de IKB-vereisten, hoewel op onderdelen de IKB-vereisten verder gaan. Denk daarbij bijvoorbeeld aan het verzamelen en verwerken van BSN's van klanten

[1] In de beleidsregel wordt de huidige beheersingsmaatregel 8.5 bij controledoelstelling 15 van het Controle Raamwerk hiervoor vervangen door de volgende beheersingsmaatregelen:

8.5 Ten minste eenmaal per jaar en daarnaast (a) na iedere wijziging van de Beleidsregel Individueel Klantbeeld en (b) na iedere wijziging in de wijze waarop de bank de beheersingsmaatregelen uit het Controle Raamwerk heeft uitbesteed aan externe dienstverleners stelt de bank vast dat er met de externe dienstverleners effectieve afspraken zijn gemaakt over de beheersingsmaatregelen uit het Controle Raamwerk die de bank heeft uitbesteed aan een of meer externe dienstverleners. Daarnaast stelt de bank dan ook vast dat dat er effectieve afspraken zijn gemaakt met de externe dienstverlener dat de dienstverlening voor zover noodzakelijk voor DGS doorloopt in het geval van faillissement.
8.6 Ten minste eenmaal per jaar stelt de bank vast dat er een of meer assurance rapportages zijn verkregen over alle beheersingsmaatregelen uit het Controle Raamwerk die de bank heeft uitbesteed aan een of meer externe dienstverleners en dat deze assurance rapportages de volledige assurance periode afdekken, of dat voor de periode waarover geen assurance is verkregen een bridge letter is ontvangen van de externe dienstverlener(s). Daarnaast stelt de bank vast dat de accountant van de externe dienstverlener heeft geconcludeerd dat de uitbestede beheersingsmaatregelen effectief hebben gewerkt gedurende de gehele assurance periode behorend bij de verkregen assurance rapportage en dat het management in de eventuele bridge letter(s) geen indicaties heeft afgegeven dat deze beheersingsmaatregelen niet langer effectief zijn.

en vertegenwoordigers of de betrouwbaarheid van gegevens die nodig zijn voor het ontdubbelen van klanten.

DNB stimuleert dat banken de synergie benutten die bestaat tussen KYC-vereisten en IKB-vereisten. De bestaande beheersingsmaatregelen kunnen worden getoetst aan de IKB-vereisten, zowel inhoudelijk als qua diepgang met het oog een de hoge mate van nauwkeurigheid die het DGS vraagt. Waar nodig kunnen deze beheersingsmaatregelen worden aangevuld. Ook IAD's kunnen hun bestaande werkprogramma's voor KYC verrijken met specifieke IKB-vereisten. De uitkomsten van de audits op KYC-processen, indien en voor zover deze uitkomsten implicaties hebben voor de naleving van IKB-vereisten, kunnen vervolgens worden meegenomen in de oordeelsvorming en het rapport over naleving van de IKB-vereisten. Daarmee wordt voorkomen dat dubbel werk wordt verricht.

h) **Nadere guidance generieke beheersingsraamwerk**
Eind 2020 heeft DNB een nieuwe versie van het generieke Controle Raamwerk gepubliceerd. Dit raamwerk wordt verder aangepast op basis van de toelichting in deze brief. De nieuwe versie wordt in april 2021 gepubliceerd op de website van DNB.

Als u naar aanleiding van deze brief vragen heeft, dan horen wij dit graag.

Met vriendelijke groet,

Mw. G.F.T. Tiellemans
Afdelingshoofd Resolutie

H.M. Kooy
Coördinator DGS