Praktijkhandreiking 1110

Code Banken: taken interne auditfunctie en externe accountant

Koninklijk Nederlands Instituut van Registeraccountants

Praktijkhandreiking 1110	
Datum:	16-03-2010
Onderwerp:	Code Banken: taken interne auditfunctie en externe accountant
Van toepassing op:	Accountants werkzaam bij banken
Status:	Praktijkhandreiking (conform NIVRA-uitingen, geeft een praktijkhandreiking uitleg en bevat dus geen nieuwe regelgeving)
Relevante wet- en regelgeving:	Algemene Maatregel van Bestuur, vastgesteld ingevolge artikel 391 lid 5 van Boek 2 van het Burgerlijk Wetboek (voorhangprocedure)

1. Inleiding

Op 9 september 2009 publiceerde de Nederlandse Vereniging van Banken de *Code Banken*. De code is gebaseerd op het op 7 april 2009 gepubliceerde rapport *Naar herstel van vertrouwen* van de Adviescommissie Toekomst Banken, de ‘commissie Maas’. De aanbevelingen over *governance* en *risk management* en de maatschappelijke rol van banken zijn verwerkt in de Code Banken. De code betreft de samenstelling, deskundigheid, taak en werkwijze van de raad van commissarissen en de raad van bestuur, het risicomanagement, de audit en het beloningsbeleid. Hiertoe behoren ook permanente educatie van de leden van de raad van commissarissen en de leden van de raad van bestuur en een door bestuurders te ondertekenen moreelethische verklaring. De code is grotendeels gebaseerd op het rapport van de commissie Maas, met uitzondering van enkele aspecten die buiten de directe invloedssfeer van de bank liggen, zoals het toezicht, vermogenseisen, het depositogarantiestelsel en de aandeelhouders. Voor wat betreft de in de code opgenomen paragraaf over het beloningsbeleid is rekening gehouden met het in mei 2009 door de Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) uitgebrachte document ‘Principes voor beheerst beloningsbeleid’.

2. Samenvatting

In de Code Banken zijn in paragraaf 5 de principes over de audit (interne auditfunctie en externe accountant) opgenomen. Deze praktijkhandreiking geeft, op basis van die principes, een nadere uiteenzetting van de werkzaamheden van de interne auditfunctie en de externe accountant. Deze praktijkhandreiking zal in 2011 geëvalueerd worden op basis van ervaringen van accountants en de sector (NVB) zelf.

Alhoewel voor de *governance* geen algemeen toetsingskader beschikbaar is zijn op deelgebieden wel normen aanwezig die accountants kunnen gebruiken bij het vormen van hun oordeel over de *governance*, het risicobeheer en de beheersprocessen binnen de bank. De interne auditfunctie rapporteert op basis van de door haar uitgevoerde beoordeling haar bevindingen aan de raad van bestuur en de auditcommissie. De externe accountant voert werkzaamheden uit in het kader van de opdracht tot controle van de jaarrekening en rapporteert zijn bevindingen over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen in zijn verslag aan de raad van bestuur en de raad van commissarissen. De werkzaamheden van de externe accountant zijn niet gericht op het formuleren van een algeheel oordeel over de *governance*, het risicobeheer en de beheersprocessen. De interne auditfunctie en de externe accountant werken hierbij nauw samen, waarbij de laatste voor zijn verslag mede gebruik maakt van de bevindingen van de interne auditfunctie. Onder ‘kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen binnen de bank’ wordt in deze Praktijkhandreiking verstaan de mate waarin de *governance*, het risicobeheer en de beheersprocessen van de bank bijdragen aan de realisatie van de daarmee beoogde doelstellingen, het op evenwichtige wijze behartigen van de belangen van alle bij de bank betrokken partijen zoals haar klanten, aandeelhouders en medewerkers, en meer in het bijzonder de beheersing van de daarmee samenhangende risico's.

3. Doel en afbakening

In deze Praktijkhandreiking worden handvatten geboden voor de interne auditfunctie en de externe accountant betreffende de taken die in de Code Banken aan hen worden toebedeeld. Bij de nadere uitwerking hiervan dient rekening te worden gehouden met het specifieke karakter van de individuele bank. Hoewel de interne auditfunctie ook aan de orde komt in andere delen van de code heeft deze Praktijkhandreiking alleen betrekking op paragraaf 5 van de code. Voor een goed begrip verdient het aanbeveling de Code Banken en deze Praktijkhandreiking te lezen in de context van het rapport van de commissie Maas.

In het kader van deze Praktijkhandreiking, waarin aandacht wordt besteed aan de samenwerking tussen de interne auditfunctie en de externe accountant alsmede de relatie tussen de auditcommissie en de interne auditfunctie, is het van belang kennis te nemen van eerdere publicaties van het NIVRA en IIA Nederland over deze samenwerking respectievelijk relatie[1].

4. Code Banken

Deze Praktijkhandreiking geeft toelichtingen op de taakopvatting van de interne auditfunctie en de externe accountant zoals weergegeven in de principes 5.3 en 5.5 uit de Code Banken:

Principe 5.3
De interne auditfunctie heeft tot taak te beoordelen of de interne beheersmaatregelen in opzet, bestaan en in werking effectief zijn. Daarbij ziet zij onder meer op de kwaliteit en effectiviteit van het functioneren van de governance, het risicobeheer en de beheersprocessen binnen de bank. De interne auditfunctie rapporteert over de bevindingen aan de raad van bestuur en de auditcommissie.

Principe 5.5
In het kader van de algemene controleopdracht voor de jaarrekening rapporteert de externe accountant in zijn verslag aan de raad van bestuur en de raad van commissarissen zijn bevindingen over de kwaliteit en effectiviteit van het functioneren van de governance, het risicobeheer en de beheersprocessen binnen de bank.

De Code Banken (hierna te noemen de code) krijgt een wettelijke verankering via een daartoe opgesteld Besluit van het ministerie van Justitie van 9 december 2009 (voorhangprocedure 'Ontwerpbesluit tot vaststelling van nadere voorschriften omtrent de inhoud van het jaarverslag van banken')[2]. Dit betekent een additionele wettelijke verplichting voor de externe accountant van de bank. De code is van kracht vanaf 1 januari 2010 en de verantwoording over het naleven van de code zal plaatsvinden in het jaarverslag van de banken over 2010. Hoewel de verantwoording pas in de eerste helft van 2011 zal plaatsvinden, zullen banken in 2010 voortvarend te werk gaan met de implementatie en naleving van de code. De interne auditfunctie zal toetsing op de naleving in 2010 gaan uitvoeren.

5. Interne auditfunctie[3]

In de code wordt ingegaan op de rol van de interne auditfunctie binnen een bank. In deel 5 van de code wordt gesteld dat de interne auditfunctie zich een oordeel moet vormen over de beheersing van de risico's die samenhangen met de activiteiten van de bank. In het oordeel van de interne auditfunctie moet de kwaliteit en de effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen binnen de bank worden meegenomen. De *governance* en het functioneren van de raad van commissarissen zullen daar waar mogelijk en wenselijk betrokken worden in de scope van de oordeelsvorming van de interne auditfunctie.

---

1 In het kader van de NIVRA-debatbijeenkomsten zijn verschenen: 'Impact op governance: Interne en externe auditor; samen een nog sterkere bijdrage aan de *governance*' en 'Bondgenoten in Governance: de relatie tussen de Auditcommissie en de Internal Audit Functie in Nederland'. Ook is het van belang kennis te nemen van Standaard 610 'Gebruikmaken van de werkzaamheden van de interne accountantsfunctie' uit de Nadere voorschriften controle en overige standaarden (NV COS).

2 Het ontwerpbesluit tot vaststelling van nadere voorschriften omtrent de inhoud van het jaarverslag van banken dateert van 9 december 2009. De voordracht voor een algemene maatregel van bestuur, vast te stellen ingevolge artikel 391 lid 5 van boek 2 van het Burgerlijk Wetboek, wordt niet eerder gedaan dan vier weken nadat het ontwerp aan de Tweede Kamer en aan de Eerste Kamer is overgelegd.

3 Deze paragraaf is in samenwerking tussen de auditcommissie van de NVB en de NIVRA Sectorcommissie Banken, Beleggingsinstellingen en –ondernemingen (SBB) opgesteld.

Vóór het van kracht worden van de Wet op het financieel toezicht (Wft) waren de belangrijkste bepalingen voor de organisatie-inrichting en risicobeheersing van een bank opgenomen in één regeling, de Regeling Organisatie en Beheersing (ROB) met bijlagen van DNB. Thans zijn deze bepalingen opgenomen in een aantal documenten. Hoewel onderstaande lijst niet uitputtend is biedt deze nu een basis voor het door de interne auditfunctie te hanteren toetsingskader:

- De Wet op het financieel toezicht (Wft).
- Het Besluit prudentiële regels Wft.
- De Praktijkhandreiking 1104 van het NIVRA.
- De Nederlandse Corporate Governance Code.
- De standaarden van het Institute of Internal Auditors (IIA).
- De Code Banken.
- Het COSO-ERM model (indien van toepassing op de organisatie).

De werkzaamheden die deel 5 van de code oplegt aan de interne auditfunctie zijn voor het overgrote deel al bestaande praktijk. De code introduceert echter een aantal nieuwe elementen waarvoor aanvullende toelichting gewenst is. Nieuwe elementen zijn:

- De eis dat de interne auditfunctie een rechtstreekse rapportagelijn heeft naar de voorzitter van de auditcommissie (zie ook de *best practices* in de relatie tussen auditcommissie en interne auditfunctie in het eerder genoemde rapport ‘Bondgenoten in Governance’).
- Het uitspreken van een oordeel over het functioneren van de *governance* van de banken door de interne auditfunctie.
- Passend binnen het kader om een oordeel uit te spreken over het functioneren van de *governance*, dient het functioneren van de raad van bestuur aan de orde te komen. Een oordeel over de raad van commissarissen zelf valt voor de interne auditfunctie buiten de scope van de code.
- De interne auditfunctie is zelf onderdeel van de *governance*. Niettemin zal daar waar dat mogelijk en wenselijk is en niet stuit op bezwaren, een toets op het functioneren van de raad van commissarissen meegenomen worden in de beoordeling van de *governance* door de interne auditfunctie. Regelgeving van het IIA geeft aan dat het verplicht is eens in de vijf jaar een externe toets te laten uitvoeren naar het functioneren van de interne auditfunctie. Hierbij komt dat ook rekening gehouden moet worden met regelgeving van het NIVRA[4].

Hieronder zal per principe uit paragraaf 5 van de code een toelichting worden gegeven.

Principe 5.1
De raad van bestuur draagt zorg voor systematische controle op de beheersing van de risico's die met de (bedrijfs)activiteiten van de bank samenhangen.

Toelichting:
Dit behoeft geen nadere toelichting.

Principe 5.2
Binnen de bank is een interne auditfunctie werkzaam die onafhankelijk is gepositioneerd. Het hoofd interne audit rapporteert aan de voorzitter van de raad van bestuur en heeft een rapportagelijn naar de voorzitter van de auditcommissie.

Toelichting:
De instelling beschikt over een interne auditfunctie die rechtstreeks onder de voorzitter van de raad van bestuur ressorteert en rechtstreeks met de voorzitter van de auditcommissie (of bij ontstentenis daarvan met de raad van commissarissen) kan schakelen.

4 Bijvoorbeeld de Verordening gedragscode (VGC), Standaard 3000 ‘Assurance-opdrachten anders dan opdrachten tot controle of beoordeling van historische financiële informatie’ en Standaard 610 ‘Gebruikmaking van de werkzaamheden van de interne accountantsfunctie’.

De interne auditfunctie beschikt over:
a. een actueel charter waarin haar taken, bevoegdheden en verantwoordelijkheden staan beschreven;
b. voldoende deskundigheid om de risico's die de bij de bank (kunnen) spelen op waarde te schatten;
c. vrije toegang tot alle activiteiten, functionarissen, locaties en informatie van de bank.

Het bovengenoemde betreft eigenlijk al bestaande praktijk. Artikel 17 van het Besluit prudentiële regels Wft stelt expliciet dat de effectiviteit van de organisatie-inrichting en van de procedures en maatregelen ten minste jaarlijks op onafhankelijke wijze wordt getoetst. Daartoe beschikt de financiële onderneming over een organisatieonderdeel dat deze interne controlefunctie uitoefent. Hiermee heeft de interne auditfunctie zijn wettelijke basis. In de Wft staat echter niet expliciet opgenomen dat het hoofd van de interne auditfunctie rapporteert aan de voorzitter van de raad van bestuur en de voorzitter van de auditcommissie. In het Besluit wordt gesteld dat onder meer tot de taken van de interne auditfunctie gerekend wordt:

"het ten minste jaarlijks rapporteren aan de personen die het dagelijks beleid van de bank bepalen en aan het orgaan, indien aanwezig, dat is belast met toezicht op het beleid en de algemene gang van zaken van de bank inzake aangelegenheden met betrekking tot de interne controle en de genomen maatregelen in geval van gesignaleerde tekortkomingen".(art. 17a, lid d.)

Het rapporteren aan de voorzitters van de raad van bestuur en de auditcommissie zal bijdragen aan de onafhankelijke positie van de interne auditfunctie.

Principe 5.3
De interne auditfunctie heeft tot taak te beoordelen of de interne beheersmaatregelen in opzet, bestaan en in werking effectief zijn. Daarbij ziet zij onder meer op de kwaliteit en effectiviteit van het functioneren van de governance, het risicobeheer en de beheersprocessen binnen de bank. De interne auditfunctie rapporteert over de bevindingen aan de raad van bestuur en de auditcommissie.

Toelichting:
Voor de beoordeling van de *governance* kan gebruik worden gemaakt van meerdere standaarden van het IIA over *control* en *governance* en het Besluit prudentiële regels Wft (de wettelijke basis voor de werkzaamheden van de interne auditfunctie). Dit besluit gaat nader in op het risicobeheer en de beheersprocessen binnen de bank, maar spreekt zich niet uit over de beoordeling van de *governance* binnen de bank. De beoordeling van de *governance* door de interne auditfunctie zal zich, tegen de achtergrond van het risicoprofiel en de risicobereidheid (*risk appetite*) van de bank, met name richten op:

- de inrichting van de organisatie (inclusief *three lines of defense*);
- de taakverdeling inclusief functiescheidingen;
- de inrichting van de *second line of defense* (waaronder *risk management*, *compliance* en);
- de inhoud van mandaten en procuratieregelingen;
- het inrichten van het integriteitsbeleid;
- het monitoren van de performance;
- het sturen op verbeterpotentieel; en
- het sanctiebeleid bij niet naleven van de regels.

Hierbij zal nadrukkelijk gekeken worden naar de voorbeeldfunctie van de raad van bestuur *(tone at the top*).

Voor de praktische uitwerking van de onderwerpen die *governance* omvatten, betekent dit dat de interne auditfunctie het auditplan en de risicoanalyse die daaraan ten grondslag liggen ter goedkeuring voorlegt aan de raad van bestuur en de auditcommissie. Periodiek rapporteert zij aan deze gremia over de voortgang van de uitvoering en de uitkomsten van de uitgevoerde audits. Daarbij toetst de interne auditfunctie ten minste jaarlijks (groepsbreed) de effectiviteit van de organisatie-inrichting en de

procedures en maatregelen gericht op de beheersing van de risico's die de bank loopt. Zij brengt daaromtrent rapport uit aan de raad van bestuur en de auditcommissie.

In bijgevoegd toetsingskader van banken worden elementen met betrekking tot kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen binnen de bank uiteengezet (**bijlage 1**).

Principe 5.4
Tussen de interne auditfunctie, de externe accountant en de risico- of auditcommissie van de raad van commissarissen vindt periodiek informatie-uitwisseling plaats. In het kader van deze informatie-uitwisseling is ook de risicoanalyse en het auditplan van de interne auditfunctie en van de externe accountant onderwerp van overleg.

Toelichting:
Dit betreft bestaande praktijk welke voortvloeit uit bovengenoemde documenten. Een dergelijk overleg vindt in de praktijk doorgaans ten minste jaarlijks plaats.

Principe 5.5
In het kader van de algemene controleopdracht voor de jaarrekening rapporteert de externe accountant in zijn verslag aan de raad van bestuur en de raad van commissarissen zijn bevindingen over de kwaliteit en effectiviteit van het functioneren van de governance, het risicobeheer en de beheersprocessen binnen de bank.

Toelichting:
Hiervoor wordt verwezen naar paragraaf 5.

Principe 5.6
De interne auditfunctie neemt het initiatief om met de Nederlandsche Bank en de externe accountant ten minste jaarlijks in een vroegtijdige fase elkaars risicoanalyse,bevindingen en auditplan te bespreken.

Toelichting:
Dit betreft in veel gevallen reeds de bestaande praktijk. Aandachtspunt is met name het vroegtijdig delen van de informatie. Dit streven loopt in lijn met de nieuwe invulling van het tripartiete overleg waarbij de interne auditfunctie, de externe accountant en de Nederlandsche Bank meerdere keren per jaar informatie met elkaar delen. Deze gesprekken, die op initiatief van de interne auditfunctie worden opgezet, passen binnen het raamwerk van de totale planning van de interne auditfunctie en de externe accountant.

Van belang is het om bevindingen, waaronder afwijkingen van de code, tijdig te bespreken met de auditcommissie en de externe accountant.

6. Externe accountant

Op basis van zijn opdracht tot controle van de jaarrekening van een kredietinstelling rapporteert de accountant in zijn verslag aan de raad van bestuur en de raad van commissarissen over zijn bevindingen met betrekking tot de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen, die hij heeft opgedaan in het kader van de algemene controleopdracht voor de jaarrekening.

De - als gevolg van de wettelijke verankering van de code ontstane - wettelijke verplichting voor de externe accountant tot het rapporteren van zijn bevindingen over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen, vloeit voort uit de opdracht tot controle van de jaarrekening. De externe accountant zet bij voorkeur in de opdrachtbevestiging de

aard van de verplichting uiteen en vermeldt dat de werkzaamheden niet zijn gericht op het formuleren van een algeheel oordeel over de *governance*, het risicobeheer en de beheersprocessen.

Gelet op de wettelijke bepalingen en de code, achten de opstellers (wetgever en banken) de rapportage door de externe accountant in zijn verslag aan de raad van bestuur en de raad van commissarissen over zijn bevindingen over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen, van belang. De wettelijke bepalingen en de code geven geen nadere omschrijving van de gehanteerde begrippen en de verwachtingen die omtrent de bevindingen bestaan.

De formulering in principe 5.5 van de code “In het kader van de algemene controleopdracht voor de jaarrekening” impliceert dat dit vereiste niet tot aanvullende werkzaamheden leidt. Hierbij dient de externe accountant in acht te nemen dat aan de werkzaamheden ten behoeve van de controle van de jaarrekening bij banken, doorgaans verdergaande eisen worden gesteld in vergelijking met andere, niet-gereguleerde, ondernemingen, onder meer als gevolg van:

- Het maatschappelijke belang van banken.
- De betrokkenheid van toezichthouders.
- Het belang van naleving van wet- en regelgeving (*compliance* en integriteit). en
- De complexiteit van bedrijfsprocessen.

Voor een uiteenzetting van de extra eisen die gesteld worden aan de werkzaamheden van de externe accountant wordt verwezen naar de NIVRA-praktijkhandreiking 1104, genaamd ‘De wettelijke verplichtingen van de accountant die de jaarrekening of de staten controleert van een financiële onderneming of een pensioenfonds’.

De externe accountant brengt gewoonlijk de bevindingen die hij opdoet bij de controle van de jaarrekening, indien en voor zover relevant voor de controle van de jaarrekening, onder de aandacht van de bestuurders en de raad van commissarissen. Deze bevindingen kunnen ook de *governance*, het risicobeheer en de beheersprocessen betreffen, voor zover deze van invloed zijn op de jaarrekening.

De externe accountant kan bij de controle van de jaarrekening ook bevindingen opdoen die niet van invloed zijn op de jaarrekening. Deze kunnen, vanuit een andere invalshoek, wel van belang zijn voor de onderneming en haar belanghebbenden. De externe accountant brengt deze op grond van de code ook onder de aandacht van de bestuurders en de raad van commissarissen. Hierbij kan gedacht worden aan:

- Samenstelling raad van bestuur en raad van commissarissen.
- Bestaan en samenstelling van verbijzonderde commissies (auditcommissie, risicocommissie).
- Vergaderfrequentie en onderwerpen van overleg bestuursorganen. en
- Risicoprofiel, risicoperceptie en risicobeheersing.

De externe accountant maakt bij zijn werkzaamheden voor de controle van de jaarrekening bij banken veelal gebruik van de werkzaamheden van de interne auditfunctie. Daartoe neemt de externe accountant onder meer kennis van de onderzoeken die door de interne auditfunctie zijn uitgevoerd die relevant kunnen zijn voor zijn oordeelsvorming over de jaarrekening. Indien en voor zover hij daarbij kennis neemt van bevindingen van de interne auditfunctie die relevant kunnen zijn voor de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen zoals bedoeld in de Code Banken, brengt hij deze ook onder de aandacht van de raad van bestuur en de raad van commissarissen.

De externe accountant baseert zich voor zijn bevindingen op algemeen aanvaarde beginselen voor de kwaliteit van de *governance*, het risicobeheer en de beheersprocessen alsmede op voor banken relevante wet- en regelgeving. Zie voor de *governance*-aandachtspunten hetgeen genoemd is bij de toelichting van principe 5.3.

Gelet op de reikwijdte van zijn werkzaamheden die bedoeld zijn om tot een oordeel over de jaarrekening te komen, doet de externe accountant geen specifiek onderzoek naar de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen. De externe accountant zal bij zijn werkzaamheden wel kennisnemen van aspecten betreffende dit onderwerp, veelal zonder dat hij daarvan een volledig beeld verkrijgt. De externe accountant draagt niettemin zorg voor een deugdelijke grondslag voor zijn (deel)bevindingen.

In **bijlage 2** zijn aandachtspunten opgenomen voor de externe accountant die de jaarrekening van een bank controleert, betreffende de Code Banken.

Bijlage 1 Aandachtspunten voor de interne auditfunctie

IIA 2110 - Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization;
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

2110.A1 - The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.

2110.A2 - The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

2110.C1 - Consulting engagement objectives must be consistent with the overall values and goals of the organization.

IIA 2130 - Control
The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2130.A1 - The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

2130.A2 - Internal auditors should ascertain the extent to which operating and program goals and objectives have been established and conform to those of the organization.

2130.A3 - Internal auditors should review operations and programs to ascertain the extent to which results are consistent with established goals and objectives to determine whether operations and programs are being implemented or performed as intended.

2130.C1 - During consulting engagements, internal auditors must address controls consistent with the engagement's objectives and be alert to significant control issues.

2130.C2 - Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

Vervolg Bijlage 1 Aandachtspunten voor de interne auditfunctie

Toetsingskader *governance* voor banken

1. De bank richt de bedrijfsvoering zodanig in dat voorzien wordt in een beheerste en integere uitoefening van haar bedrijf.

2. De bank heeft een goed overzicht van en inzicht in het reilen en zeilen van alle groepsonderdelen die in materieel opzicht relevant zijn.

3. De bank kent een duidelijke en adequate organisatiestructuur die een goede interne beheersing faciliteert.

4. De organisatie-inrichting en de wijze waarop invulling wordt gegeven aan de interne beheersing van de *key*-bedrijfsprocessen zijn systematisch en toegankelijk vastgelegd.

5. De bank houdt intern periodiek de strategie en de doelstellingen tegen het licht, past deze zo nodig aan op basis van veranderende omstandigheden en deelt de uitkomsten hiervan met haar medewerkers.

6. De bank beschikt over helder geformuleerde beleidsuitgangspunten die gericht zijn op risicobeheersing en integer handelen.

7. De bank zorgt voor een systematisch uit te voeren risicoanalyse gericht op het identificeren, meten en evalueren van alle relevante bedrijfsrisico's.

8. De risicoanalyse wordt uitgevoerd of begeleid door deskundigen die onafhankelijk zijn van de functies die verantwoording afleggen over de commerciële en/of financiële prestaties van de bank.

9. De bank voert beleid gericht op het beheersen van relevante risico’s. Onder relevante risico’s, worden in het bijzonder verstaan het concentratierisico, krediet- en tegenpartijrisico, liquiditeitsrisico, marktrisico, operationeel risico, renterisico voortvloeiend uit niet handelsactiviteiten, restrisico, securitisatierisico en verzekeringsrisico. De bank houdt tevens rekening met de risico’s die voortvloeien uit de macro-economische omgeving waarin zij opereert en die verband houden met de stand van de conjunctuurcyclus.

10. De bank draagt zorg voor de uitwerking en implementatie van de beleidsuitgangspunten in organisatorische en administratieve procedures en maatregelen.

11. De procedures en maatregelen bestaan onder meer uit autorisatieprocedures, limietstellingen, limietbewaking en procedures en maatregelen voor noodsituaties en zijn afgestemd op de aard, de omvang, het risicoprofiel en de complexiteit van de werkzaamheden van de bank.

12. De bank draagt zorg voor een systematisch toezicht op de naleving van organisatorische en administratieve procedures en maatregelen die gericht zijn een adequate risicobeheersing en integer handelen.

13. De bank beschikt over een onafhankelijke risicobeheerfunctie die op systematische wijze een onafhankelijk risicobeheer uitvoert dat gericht is op het identificeren, meten en evalueren van de risico’s waaraan de bank is of kan worden blootgesteld.

14. De bank draagt zorg voor een eenduidige verdeling van taken, verantwoordelijkheden en bevoegdheden en daarop afgestemde rapportagelijnen en heeft deze systematisch vastgelegd.

15. De bank zorgt voor toereikende functiescheidingen om in een beheerste en integere bedrijfsvoering te voorzien.

16. De bank zorgt ervoor dat de rechten en verplichtingen die door de bank worden aangegaan administratief goed worden vastgelegd.

17. De bank beschikt over een adequaat systeem van informatievoorziening waarbij de uitkomsten van de bedrijfsvoering goed worden vastgelegd en gerapporteerd, zodanig dat tijdig inzicht bestaat in de (groepsbreed) gelopen risico's.

18. De bank beschikt over (beschreven) procedures en maatregelen die moeten voorkomen dat er oneigenlijk gebruik gemaakt wordt van informatie.

19. De bank beschikt over (beschreven) procedures en maatregelen die het ongestoord en betrouwbaar functioneren van de kritische bedrijfsprocessen waarborgen. Deze zijn gericht op:
    a. het beheersen van de bedrijfsprocessen en bedrijfsrisico's;
    b. het borgen van de integriteit van haar medewerkers en klanten om te voorkomen dat het vertrouwen in de bank of de financiële markten ernstig kan worden geschaad;
    c. het zekerstellen van de soliditeit van de bank.

20. De bank draagt zorg voor een systematische toetsing en beoordeling van de interne beheersing. Dit kan plaatsvinden door het lijnmanagement (*first line of defense*), groepsonderdelen die opgesteld staan voor de adequate beheersing van de risico's (zoals *control, compliance* en *risk management* als zijnde de *second line of defense*) of de interne auditfunctie.

21. De opdracht van de bank aan de externe accountant tot onderzoek van de jaarrekening voorziet in een toetsing en beoordeling op hoofdlijnen met betrekking tot de toereikendheid van de organisatie-inrichting en risicobeheersing.

22. De raad van bestuur maakt duidelijk wie binnen dat gremium primair verantwoordelijk is voor elk van de te onderscheiden risicogebieden.

23. De raad van bestuur draagt zorg voor het uitdragen van de bankeigen normen en waarden. businessethiek vormt hier een belangrijk onderdeel van. Dit onderwerp is weer een onderdeel van het permanente educatieprogramma van de raad van bestuur.

24. De raad van bestuur draagt er zorg voor dat:
    a. zijn taakverdeling en werkwijze in een reglement zijn vastgelegd;
    b. hij regelmatig (ten minste vierwekelijks) vergadert;
    c. schriftelijk verslag doet van zijn vergaderingen.

25. De raad van bestuur draagt er zorg voor dat de uitgangspunten als verwoord in de Nederlandse Corporate Governance Code worden nagekomen.

26. De raad van bestuur draagt er zorg voor dat de bepalingen als opgenomen in de Code Banken worden nagekomen.

27. De raad van bestuur draagt er zorg voor dat in het jaarverslag melding gemaakt wordt dat de interne risicobeheersings- en controlesystemen een redelijke mate van zekerheid geven dat de

financiële verslaggeving geen onjuistheden van materieel belang bevat en dat deze systemen in het verslagjaar naar behoren hebben gewerkt.

28. De raad van bestuur draagt er zorg voor dat elke (schijn van) verstrengeling tussen de privébelangen of andere functies van zijn leden en de zakelijke belangen van de bank wordt vermeden.

29. De raad van bestuur draagt er zorg voor dat de raad van commissarissen tijdig beschikt over alle relevante interne en externe informatie die noodzakelijk is voor de uitoefening van zijn wettelijke en statutaire taken.

Bijlage 2: Aandachtpunten voor de externe accountant

Inleiding
In deze bijlage zijn aandachtspunten betreffende de Code Banken opgenomen voor de externe accountant die de jaarrekening van een bank controleert.

Doel
Deze bijlage is een hulpmiddel bij het signaleren en rapporteren door de externe accountant van bevindingen over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen. De inhoud is niet uitputtend. De externe accountant zal zijn werkzaamheden aanpassen aan de specifieke omstandigheden.

Normen
De externe accountant baseert zich voor zijn bevindingen op algemeen aanvaarde beginselen voor de kwaliteit van de *governance*, het risicobeheer en de beheersprocessen alsmede op voor banken relevante wet- en regelgeving.

Banken met een vergunning zoals bedoeld in de Wft dienen de bepalingen van en ingevolge de Wft na te leven. Bepaalde aspecten betreffende *governance*, risicobeheer en beheersprocessen worden behandeld in:

- Wet op het financieel toezicht (Wft), Hoofdstuk 3.3 Regels voor het werkzaam zijn op de financiële markten
  - Afdeling 3.3.2 Deskundigheid, betrouwbaarheid en integriteit
  - Afdeling 3.3.3 Structurering en inrichting
  - Afdeling 3.3.4 Overige bepalingen

- Besluit prudentiële regels Wft (Bpr)
  - Hoofdstuk 3 Integere uitoefening van het bedrijf
  - Hoofdstuk 4 Beheerste uitoefening van het bedrijf
  - Hoofdstuk 5 Uitbesteding van werkzaamheden

De bepalingen waarnaar hierboven verwezen wordt zijn bij de totstandkoming van de Wft gebaseerd op de meer gedetailleerde bepalingen van regelingen van de Nederlandsche Bank. Hoewel deze regelingen bij de invoering van de Wft zijn vervallen, geven zij een goed beeld van hetgeen met de bepalingen van de Wft en het Bpr wordt bedoeld. Het betreft de volgende regelingen.

- Regeling organisatie en beheersing.
- Regeling bestuurderskredieten.
- Regeling afgeschermde rekeningen.
- Regeling incidenten kredietinstellingen en verzekeraars.
- Regeling integriteitsgevoelige functies.
- Regeling CDD kredietinstellingen.

In de Nederlandse Corporate Governance Code zijn de normen vastgelegd die van toepassing zijn op zogenoemde beursvennootschappen:

- Vennootschappen met statutaire zetel in Nederland waarvan de aandelen of certificaten van aandelen zijn toegelaten tot een effectenbeurs, of meer specifiek tot de handel van een gereglementeerde markt of een daarmee vergelijkbaar systeem.
- Grote vennootschappen met statutaire zetel in Nederland (> € 500 miljoen balanswaarde) waarvan de aandelen of certificaten zijn toegelaten tot de handel op een multilaterale handelsfaciliteit of een daarmee vergelijkbaar systeem.

met uitzondering van:

- Beleggingsmaatschappijen die geen beheerder zijn in de zin van artikel 1:1 Wft.

Houders van aandelen worden gelijk gesteld met houders van certificaten van aandelen welke met medewerking van de vennootschap zijn uitgegeven.

Andere bronnen zijn:

- The Principles of Corporate Governance - Organisation for Economic Co-operation and Development (OECD)
- Internal Control Framework - Committee of Sponsoring Organizations of the Treadway Commission (COSO);
- Enhancing corporate governance for banking organisations - Bank for International Settlements (BIS).

De principes van de Code Banken waarmee de externe accountant bij de controle van de jaarrekening kan worden geconfronteerd betreffen de volgende onderwerpen.

- Een bank vermeldt volgens de code elk jaar in haar jaarverslag op welke wijze zij de principes van de code in het voorafgaande jaar heeft toegepast en zet, indien van toepassing, gemotiveerd uiteen waarom een principe eventueel niet (volledig) is toegepast. De externe accountant toetst ingevolge artikel 2:393 lid 5 onder f BW of het jaarverslag, voor zover hij dat kan beoordelen, verenigbaar is met de jaarrekening. Wanneer hem informatie bekend is op grond waarvan hij tot de conclusie komt dat de weergave over de toepassing van de principes in het (concept)jaarverslag onjuist is, maakt hij dat kenbaar aan de raad van bestuur en de raad van commissarissen.
- Van de externe accountant mag worden verwacht dat hij bij zijn werkzaamheden kennis neemt van de samenstelling van de raad van commissarissen en de raad van bestuur en deze zou kunnen toetsen aan de principes van de code. De deskundigheid van de leden van de raad van commissarissen en de raad van bestuur is in het kader van zijn werkzaamheden nauwelijks toetsbaar door de externe accountant. De externe accountant zal over de deskundigheid daarom geen bevindingen kunnen melden. De externe accountant neemt ook in zekere mate kennis van de taken en werkwijzen van de raad van commissarissen en de raad van bestuur en zal deze ten dele kunnen toetsen aan de principes van de code.
- Het risicomanagement behoort tot het aandachtsgebied van de externe accountant voor zover het van betekenis is voor de financiële verantwoording. Omdat gebrekkig risicomanagement niet alleen van directe invloed kan zijn op de cijfers maar ook indirect van financiële betekenis kan zijn (bijvoorbeeld door aantasting van de goede naam van de bank hetgeen kan leiden tot bedreiging van de continuïteit, boetes door toezichthouders of intrekken van de vergunning) zal de externe accountant doorgaans ruime aandacht geven aan risicobeheersing.
- Het beloningsbeleid als zodanig is geen aandachtsgebied van de externe accountant bij de controle van de jaarrekening. Bij onderzoek naar individuele beloningen zal de externe accountant niettemin kunnen vaststellen of deze zijn vastgesteld binnen het daartoe bepaalde beleid, waarbij tevens aandacht kan worden besteed aan ‘retentie-, exit- en welkomstpakketten’ zoals genoemd in de code.

Gebruikmaken van de werkzaamheden van de interne auditfunctie

Banken beschikken doorgaans over een interne auditfunctie waarvan de externe accountant bij het uitvoeren van zijn werkzaamheden voor de controle van de jaarrekening gebruik maakt. De externe accountant neemt kennis van de door de interne auditfunctie uitgevoerde werkzaamheden en toetst de kwaliteit en de bruikbaarheid van deze werkzaamheden voor zijn onderzoeksdoel. Wanneer hij hierbij kennis neemt van informatie over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen, brengt hij deze (ook) onder de aandacht van de raad van bestuur en de raad van commissarissen.

De interne auditfunctie vervult een specifieke rol in de Code Banken. Volgens principe 5.3 heeft de interne auditfunctie tot taak te beoordelen of de interne beheersmaatregelen in opzet, bestaan en in werking effectief zijn. Daarbij ziet zij volgens de code onder meer op de kwaliteit en effectiviteit van

het functioneren van de *governance*, het risicobeheer en de beheersprocessen binnen de bank. De interne auditfunctie rapporteert over de bevindingen aan de raad van bestuur en de auditcommissie.

De externe accountant van een bank neemt kennis van de uitkomsten van deze beoordeling en bespreekt deze met de interne auditfunctie. De externe accountant stelt vast dat belangrijke bevindingen van de interne auditfunctie onder de aandacht van de raad van bestuur en de auditcommissie zijn gebracht. Wanneer de externe accountant kennis neemt van belangrijke beperkingen of gebreken bij de uitvoering van de werkzaamheden door de interne auditfunctie, dan brengt hij deze bevindingen ook onder de aandacht van de raad van bestuur en de raad van commissarissen.

Bij zijn werkzaamheden neemt de externe accountant in acht dat de reikwijdte van de werkzaamheden van de interne auditfunctie beperkt is tot de bank en haar raad van bestuur. De reikwijdte van het begrip *governance* van de Code Banken is ruimer en omvat mede de raad van commissarissen en haar commissies.

Rapportage over bevindingen
De externe accountant rapporteert volgens de code in zijn verslag (brief van bevindingen of *management letter*) aan de raad van bestuur en de raad van commissarissen over zijn bevindingen over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen. Daarenboven heeft de externe accountant met enige regelmaat contact en overleg met de raad van bestuur, de raad van commissarissen en/of de auditcommissie. Tijdens dit overleg worden de bevindingen zoals hiervoor bedoeld ook aan de orde gesteld.

Voorbeeldtekst aanvullende paragraaf opdrachtbrief

Ingevolge de (wettelijke bepalingen) / Code Banken rapporteert de externe accountant in het kader van de algemene controleopdracht voor de jaarrekening in zijn verslag aan de raad van bestuur en de raad van commissarissen zijn bevindingen over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen.

Wij zijn met u overeengekomen dat wij de bevindingen die wij opdoen bij het uitvoeren van onze controlewerkzaamheden over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen, aan de raad van bestuur en de raad van commissarissen zullen rapporteren. Gelet op de reikwijdte van onze werkzaamheden die bedoeld zijn om tot een oordeel over de jaarrekening te komen, zullen wij geen algeheel oordeel formuleren over de kwaliteit en effectiviteit van het functioneren van de *governance*, het risicobeheer en de beheersprocessen.

Wij rapporteren deze bevindingen zoals nader is omschreven in de Praktijkhandreiking 1110 ‘Code Banken: taken interne auditfunctie en externe accountant’, uitgegeven door het Koninklijk Nederlands Instituut van Registeraccountants.”