

De Risicoparagraaf: wat moet er in?

Door drs. Berry van Blijderveen RA en drs. Marinus de Pooter RA CMA CFM CIA

Effectief risicomanagement wordt gezien als een voorwaarde voor goed ondernemingsbestuur. In Nederland zijn de corporate governance-beginselen vastgelegd in de Code Tabaksblad. In de best practice-bepalingen II.1.3, II.1.4, II.1.5 en II.1.8 onderstreept de code het belang van een goed risicobeheersings- en controlesysteem en beschrijft hij de wijze waarop een onderneming daarvan verslag zou moeten doen in haar jaarverslag.

De commissie-Frijns plaatst in haar onderzoek naar de naleving van de Nederlandse Corporate Governance Code een aantal kanttekeningen bij de praktijk van risicoverslaggeving in het jaarverslag. Het NIVRA heeft zich in de publicatie 'Risk management and internal control systems' ook gemengd in het debat over de rol en inhoud van de risicoparagraaf. Reden genoeg om na te gaan welke eisen er worden gesteld aan de inhoud van de risicoparagraaf.

Risicoparagraaf

De risicoparagraaf is vooral bedoeld om de gebruikers van de jaarrekening te ondersteunen in (economische) beslissingen door het opnemen van betekenisvolle informatie over de significante specifieke risico's die de realisatie van de ondernemingsdoelstellingen bedreigen, alsmede de wijze waarop en de mate waarin deze worden beheerst.

Centraal in de risicoparagraaf staan de interne risicobeheersings- en controlesystemen ('IRB&CS'). Over wat deze termen precies inhouden bestaat onduidelijkheid. Ze worden in de Code Tabaksblad zowel enkelvoudig als meervoudig gebezigd en er worden slechts enkele 'instrumenten' hiervan nader toegelicht, waaronder risicoanalyses en gedragscodes. Gebruikt als meervoud kan het de verzamelterm zijn voor alle

maatregelen, inclusief monitoring-instrumenten, die het management heeft genomen voor het beheersen van de ondernemingsrisico's: het organisatie-specifieke beheersraamwerk.

De reikwijdte van de in de risicoparagraaf op te nemen managementverklaring, het in control statement ('ICS'), wordt bepaald langs de volgende dimensies:

- ▶ soort risico's: strategische, operationele, wet- en regelgevings- of alleen financiële verslaggevingsrisico's;
- ▶ conclusie over de effectiviteit: alleen ten aanzien van de opzet/het bestaan, of ook ten aanzien van de werking van de IRB&CS;
- ▶ de tijdsperiode waarover of het tijdstip waarop de conclusie betrekking heeft.

Uitgangspunten

Enkele belangrijke uitgangspunten en richtlijnen van de Code Tabaksblad, de monitoring-commissie-Frijns, de NIVRA taskforce on internal control, alsmede overige best practices met betrekking tot de risicoparagraaf zijn als volgt.

- ▶ De risicoparagraaf bevat zodanige betekenisvolle, 'high-level' informatie dat de belanghebbenden de belangrijkste elementen van de IRB&CS kunnen begrijpen.
- ▶ Bij voorkeur wordt deze informatie op één plaats in het jaarverslag opgenomen, te weten in een afzonderlijke risicoparagraaf.
- ▶ De Code Tabaksblad verlangt een 'duidelijke onderbouwing' van de managementverklaring dat de IRB&CS effectief zijn.
- ▶ De risicoparagraaf mag geen misleidende indruk geven of strijdig zijn met de overige gepresenteerde informatie in de jaarrekening.
- ▶ Het is belangrijk om de informatie in de

risicoparagraaf voor de lezer van de jaarrekening te presenteren op een wijze die haar in de tijd vergelijkbaar maakt.

Inhoud

Er is geen voorgeschreven sjabloon voor de risicoparagraaf. De volgende indeling kan gevolgd worden:

- a. inleiding (inclusief uiteenzetting van de risicomanagementfilosofie);
- b. risicoprofiel (beschrijving van de voornaamste risicocategorieën en gekozen maatregelen);
- c. IRB&CS (beschrijving van de voornaamste componenten);
- d. managementverklaring (uitspraak van het management over de effectiviteit van de IRB&CS).

a. Inleiding

In de inleiding wordt een toelichting gegeven op de risicomanagementfilosofie en risicobereidheid van het management. Welke risico's is het bestuur bereid te nemen om de ondernemingsdoelstellingen te realiseren? Dit betreft een nadere uiteenzetting van de typen specifieke risico's die het bestuur wil nemen en de aanvaardbaar geachte mate van blootstelling hieraan (risicobereidheid en risicotoleranties, zo mogelijk gekwantificeerd door middel van een gevoeligheidsanalyse). Dit zet tevens de toon voor het type beheersmaatregelen dat wordt getroffen. Het is aan te bevelen om in dit verband ook uit te leggen dat de IRB&CS zijn bedoeld om het risico dat de ondernemingsdoelstellingen niet worden gehaald te managen (dat wil zeggen, te brengen binnen de risicobereidheid van de raad van bestuur) en niet om ze te elimineren.



b. Risicoprofiel

Het risicoprofiel bestaat uit een beschrijving van de significante geïdentificeerde risico's (risicocategorieën), zo veel mogelijk gekoppeld aan de (strategische, operationele, financiële verslaggevings- en compliance) doelstellingen. Het doel van deze uiteenzetting is inzicht geven in de wijze waarop deze categorieën van onzekere toekomstige gebeurtenissen een bedreiging vormen voor de realisatie van de ondernemingsdoelstellingen. Het is aan te bevelen om van deze risico's de potentiële effecten te beschrijven, indien mogelijk met een kwantitatieve toelichting in de vorm van gevoeligheidsanalyses (ten aanzien van de omzet, het resultaat, het eigen vermogen, et cetera). De commissie-Frijns benadrukt terecht het belang van het kwantificeren van risico's voor het inzicht van de lezers van de risicoparagraaf.

De lezers van het jaarverslag willen uiteraard ook weten op welke wijze de geïdentificeerde risico's beantwoord worden. Het is daarom van belang om – op hoofdlijnen – per risicocategorie de wijze te beschrijven waarop de beheersing van deze risico's plaatsvindt (de risicobeantwoordingsstrategieën, bijvoorbeeld verzekeren, accepteren of afstoten).

c. Interne risicobeheersings- en controlesystemen

Met betrekking tot de interne risicobeheersings- en controlesystemen is het de bedoeling dat het bestuur:

- ▶ beschrijft hoe deze aansluiten bij het risicoprofiel en ingebed zijn in de organisatie (de verdeling van de verantwoordelijkheden, integratie met de plannings- en controlecyclus, etc.);
- ▶ aangeeft dat er gedurende het verslagjaar een voortdurend proces is

geweest voor het identificeren, analyseren, valideren, monitoren en evalueren van de significante risicogebieden en de getroffen beheersmaatregelen, alsmede het communiceren en rapporteren erover;

- ▶ aangeeft dat de bij het analyseren en monitoren naar voren komende mogelijke en geconstateerde zwakheden (blootstelling vanwege inadequate en ineffektieve beheersmaatregelen) worden beoordeeld en gecorrigeerd;
- ▶ het voorbehoud opneemt dat niet kan worden uitgesloten dat risico's die momenteel niet onderkend worden, dan wel nu als niet-materieel worden beschouwd, later een belangrijk negatief effect kunnen hebben op het vermogen van de onderneming om haar bedrijfsdoelstellingen te realiseren, en verder dat de interne rapporteringssystemen mede gericht zijn op tijdige identificatie van deze risico's;
- ▶ een beschrijving geeft van de belangrijkste organisatiespecifieke borgingssystemen, de IRB&CS, aansluitend bij het hiervoor beschreven risicoprofiel. Voorbeelden zijn: beschreven organisatiestructuur, delegering van bevoegdheden, managementcontracten, functiescheiding, de plannings- en controlecyclus, tijdige registratie van transacties, risicoanalyses, informatiebeveiligingsmethodiek, erkende kwaliteitsborgingssystemen (zoals voor gezondheid, veiligheid en milieu), het verzamelen en verspreiden van 'best practice controls', handleidingen voor de financiële verslaggeving, autorisatieregels, (verzekerings) portefeuillemanagement, risicofuncties en risicocommissies, managementrapportages ('balanced scorecard') met relevante sleutel-

indicatoren, crisismanagement, periodieke monitoring ('business reviews'), bijzondere onderzoeken, gedragscodes en klokkenluidersregelingen;

- ▶ uiteenzet hoe de verantwoordelijkheden (centraal versus decentraal) voor de IRB&CS zijn geregeld binnen de organisatie. Het betreft het ontwerp, de invoering, inbedding, monitoring, verificatie en evaluatie ervan;
- ▶ opneemt dat de werking van de IRB&CS gedurende het verslagjaar regelmatig is beoordeeld door de raad van bestuur en de raad van commissarissen;
- ▶ vermeldt dat het volgende is besproken met de raad van commissarissen/het audit committee:
 - a. de strategie van de onderneming;
 - b. de voornaamste risico's verbonden aan het realiseren van de ondernemingsdoelstellingen;
 - c. de uitkomsten van de evaluatie van het ontwerp en de werking van de IRB&CS, gericht op het realiseren van de doelstellingen van de onderneming;
- ▶ het voorbehoud opneemt dat de IRB&CS geen absolute zekerheid kunnen verschaffen vanwege de inherente beperkingen zoals: onvoorziene omstandigheden, menselijke beoordelingsfouten, samenspanning door medewerkers, schendingen van voorschriften, kostenbatenafwegingen en samenloop van op zich geringe oorzaken met grote gevolgen. Eventueel kan men hier aanvullen dat voor de inhoud van een 'redelijke mate van zekerheid' uitgegaan dient te worden van wat geldt voor een zorgvuldig handelende bestuurder in de gegeven omstandigheden;
- ▶ aangeeft dat de IRB&CS de effecten van



risico's op de vennootschap en haar belanghebbenden beogen te beperken, als het voorkomen van waardevermindering door blootstelling aan die risico's niet mogelijk is;

- ▶ ter onderbouwing van de managementverklaring (zie onder D) duidelijk het proces weergeeft dat is gevolgd om de effectiviteit van de werking van de IRB&CS vast te stellen. Voorbeelden zijn het gebruik van analyses, tussentijdse evaluaties, zelfbeoordelingen, interne bevestigingsbrieven, uitkomsten van interne en externe reviews, audits en collegiale toetsing, issue-escalatierapportages, et cetera;
- ▶ in het kader van het evaluatieproces verwijst naar een algemeen geaccepteerd referentiekader (standaard) dat is gebruikt voor het inrichten en toetsen van de IRB&CS, bijvoorbeeld COSO;
- ▶ indien van toepassing, tevens het proces toelicht dat is gevolgd voor het omgaan met materiële aspecten van interne beheersing die samenhangen met aanzienlijke problemen die in de jaarrekening worden vermeld.

d. Managementverklaring

De risicoparagraaf mondt uit in de managementverklaring. Hierin wordt opgenomen dat de raad van bestuur verantwoordelijk is voor adequate IRB&CS en voor het beoordelen van de effectiviteit ervan, en dat hij deze verantwoordelijkheden is nagekomen.

Welke verklaring wordt het bestuur geacht op te nemen over de effectiviteit van de IRB&CS?

Volgens de monitoring-commissie-Frijns betekent dit:

- ▶ ten aanzien van financiële verslaggevingsrisico's:
 - verklaren dat de IRB&CS een redelijke mate van zekerheid verschaffen dat de financiële verslaggeving over het verslagjaar geen onjuistheden van materieel belang bevat (en dus betrouwbaar is);
 - verklaren dat de IRB&CS naar behoren hebben gewerkt gedurende het verslagjaar (positieve assurance met betrekking tot opzet/bestaan en werking);
 - verklaren dat er geen indicaties zijn dat de IRB&CS niet naar behoren zullen werken gedurende het lopende jaar;
 - alle belangrijke tekortkomingen in de IRB&CS opsommen die gedurende het verslagjaar zijn geconstateerd, evenals belangrijke wijzigingen (in de IRB&CS) die zijn doorgevoerd en verbeteringen die zijn gepland om de geconstateerde zwakheden te herstellen;
 - ▶ ten aanzien van alle overige (strategische, operationele en wet- en regelgevings) risico's een beschrijving:
 - van de opzet en werking van de IRB&CS met betrekking tot de voornaamste risico's zoals die zich in het boekjaar konden voordoen;
 - van belangrijke tekortkomingen in de IRB&CS - voor zover van toepassing - die gedurende het verslagjaar zijn geconstateerd, evenals van significante wijzigingen (in de IRB&CS) die zijn doorgevoerd en verbeteringen die zijn gepland om de geconstateerde zwakheden te herstellen.
- Bij de variant met bredere scope (conform COSO) verklaart het bestuur dat:
- ▶ rekening houdend met genoemde

beperkingen die noodzakelijkerwijs verbonden zijn aan alle IRB&CS;

- ▶ met inachtneming van de genoemde mogelijkheden tot verbetering ervan;
- ▶ gedurende het verslagjaar (en tot het moment van het publiceren van deze verklaring);

de IRB&CS het bestuur een redelijke mate van zekerheid geven dat:

- ▶ het bestuur (tijdig) op de hoogte is van de mate waarin de strategische en operationele doelstellingen van de vennootschap worden gerealiseerd;
- ▶ de in- en externe rapportages betrouwbaar zijn;
- ▶ door de vennootschap de relevante wet- en regelgeving wordt nageleefd.

Tenslotte is het aan te bevelen nadere uitleg te geven als een van bovenstaande 'disclosures' niet kan worden gegeven.

Voor nadere informatie kunt u contact opnemen met:

Berry van Blijderveen
 Directoraat Vaktechniek
berry.van.blijderveen@nl.ey.com
 010-4068301

Marinus de Pooter
 ERM solution leader
 Netherlands
 010-406 82 68
marinus.de.pooter@nl.ey.com