PRACTICE GUIDE

‘VOR EN DE INTERNAL AUDITFUNCTIE’

Instituut van
Internal Auditors
Nederland

Inhoud

Practice Guide 'VOR en de Internal Auditfunctie'

Deze Practice Guide is in een aantal iteraties tot stad gekomen na een brede consultatie van leden (m.n. hoofden audit), partners van het IIA, andere beroepsverenigingen, commissarissen en schragende partijen.

De VOR is formeel nog niet definitief opgenomen als onderdeel van de Code; deze Practice Guide is zodoende een interpretatie van de huidige status.

1. Inleiding

De veel besproken verklaring omtrent risicobeheersing (VOR) gaat er komen. De schragende partijen van de Nederlandse Corporate Governance Code (Code) en het NBA zijn het in de werkgroep Van Manen eens geworden: in de Code zal worden opgenomen dat beursgenoteerde vennootschappen over het boekjaar beginnend op of na 1 januari 2025 een VOR (nieuwe stijl) moeten opnemen in het bestuursverslag.

In de VOR legt het bestuur verantwoording af over de opzet en werking én over de beoordeling van de effectiviteit van de risicobeheersing (ofwel de interne risicobeheersings- en controlesystemen (IRCS)) en verklaart zij welke mate van zekerheid deze systemen bieden. Daarmee komt risicobeheersing nadrukkelijker op de agenda van bestuurders en toezichthouders van beursgenoteerde vennootschappen en mag een stimulans voor de kwaliteit van risicobeheersing worden verwacht.

Doel is om met de verplichting tot publicatie van de VOR de kwaliteit van risicobeheersing en het inzicht in de organisatie te verbeteren.

De implementatie van de VOR kan voor organisaties een grote aanpassing van de IRCS betekenen. Deze practice guide van IIA Nederland beoogt handvatten te bieden, aan bestuurders, commissarissen én hoofden IAF, voor de organisatiespecifieke implementatie van de VOR, met name ook ten aanzien van de rol die de Internal Auditfunctie (IAF) hierbij kan spelen. Van oudsher is het onafhankelijk beoordelen en helpen verbeteren van de kwaliteit van de risicobeheersing een kerntaak van de IAF[1]. Vanuit die positie, vaardigheden én opgedane kennis, kan de IAF met audits en advies de organisatie ondersteunen.

In deze practice guide wordt eerst ingegaan op de VOR en haar betekenis. Daarna wordt ingegaan op de taakverdeling en enkele handvatten om die te concretiseren. Tenslotte worden de mogelijke rollen van de IAF beschreven en worden handvatten gegeven bij belangrijke keuzes om de VOR op effectieve en efficiënte wijze te kunnen onderbouwen.

Plan is dat in 2026 over het boekjaar 2025 de eerste VOR opgenomen wordt in het bestuursverslag.

Omdat alle schragende partijen er achter staan, is de verwachting dat als de nieuwe Monitoring Commissie is benoemd, het huidige voorstel in de Code wordt verwerkt. De implementatie dient dus voortvarend te worden opgepakt.

1 Ofwel de effectiviteit van governance, risicomanagement en beheersing, zoals dit in de IIA-standaarden wordt genoemd.

2. Wat vereist de VOR?

Allereerst geven we in paragraaf 2.1. een toelichting op wat de VOR nu is, in de vorm van de belangrijkste wijzigingen van de Code. In 2.2 wordt aangegeven welke acties daartoe zijn vereist.

2.1 Wat staat er in het voorstel van de schragende partijen en NBA?

Samenvattend kan worden gesteld dat de verantwoordelijkheid van het bestuur voor het identificeren en beheersen van risico's niet is gewijzigd (principe 1.2). Gewijzigd zijn met name datgene waar verantwoording over moet worden afgelegd (1.4.2) en de verklaring over de effectiviteit van de beheersing (1.4.3).

De belangrijkste wijzigingen zijn:

- Het verduidelijken van de verantwoordelijkheid van het bestuur om jaarlijks de ***effectiviteit*** van de risicobeheersings- en controlesystemen m.b.t. de operationele, compliance, en verslaggeving (financiële en duurzaamheidsverslaggeving)te beoordelen, aan de hand van een door de vennootschap zelf gekozen raamwerk. In het bestuursverslag dient het bestuur verantwoording af te leggen over die beoordeling (1.4.2).
- Het inperken van de reikwijdte van de verantwoording (1.4.2): nu exclusief strategische risico's.
- Het expliciteren dat risicobeheersing ook toeziet op duurzaamheidsinformatie.
- Het uitbreiden van de reeds bestaande bestuursverklaring (1.4.3) – niet zijnde een In-control verklaring (in de betekenis van een effectiviteitsconclusie) – met een uitspraak over de mate van zekerheid die de IRCS geven over het bereiken van de doelstellingen ten aanzien van duurzaamheidsverslaggeving[2], compliance en operations, naast financiële verslaggeving.
- Het uitbreiden van het verslag van (en daarmee de beoordeling door) de auditcommissie (1.5.3) met de onderbouwing van de VOR.

De volledige tekst van het voorstel kunt u HIER vinden; een overzicht van de belangrijkste wijzigingen t.o.v. de huidige tekst, en duiding daarvan, staat in bijlage 1.

2.2 Wat betekent dat: welke acties zijn vereist?

De VOR moet organisatie-specifiek worden ingevuld, passend bij het principle-based karakter van de Code. De mate waarin de vereisten van de nieuwe VOR aansluiten bij de huidige praktijk zal verschillen per organisatie. Voor organisaties met een volwassen systematiek van risicomanagement, zullen de veranderingen waarschijnlijk beperkt zijn. Daar waar dat niet zo is, zal de implementatie aanpassingen in de IRCS vereisen en daardoor naar verwachting enige tijd kosten.

De VOR zal niet alleen de dialoog tussen bestuurders en commissarissen (met name auditcommissie) over goed ondernemingsbestuur v.w.b. risico's en de beheersing daarvan versterken, maar ook de dialoog van de organisatie met haar stakeholders op dit vlak.
Er dienen keuzes te worden gemaakt. Het is daarbij belangrijk om het einddoel voor ogen te houden: *over welke risico's zal welke mate van zekerheid worden gegeven?*

2 Opgemerkt word dat hiervoor wordt verwezen naar de CRSD, waarin naast de rapportage van de diverse informatie-elementen ook een rapportage over de governance, inclusief de risicobeheersing en interne controle wordt vereist.

Belangrijke keuzes van de basiselementen van de VOR zijn achtereenvolgens:

- De **materialiteit** van de voor de organisatie geldende risico's: welke risico's kunnen een materiële invloed hebben op het succes van de organisatie? De Code spreekt (1.4.2) over de 'voornaamste' risico's.
- De **kwalificatie** of verwoording van de (mate van) 'zekerheid' die de beheersing van de operationele en compliance risico's geeft, ofwel de effectiviteit van deze IRCS. Het begrip 'effectiviteit' wordt wel gedefinieerd voor de financiële verslaggeving (redelijke mate van zekerheid) en duurzaamheidsverslaglegging (beperkte mate van zekerheid), maar niet voor de operationele en compliance risico's. Daar zegt men slechts wat het niet is. Juist op deze risico's is een passende bewoording lastig, gegeven de veelheid van risico-variabelen, waarbij het zowel om de effectiviteit als de efficiency van de bedrijfsvoering gaat.

  Aandachtspunten bij het bepalen van de mate van zekerheid zijn:

  - De aansluiting met de risicobereidheid van de organisatie;
  - De vermelding van de inherente beperkingen van dergelijke systemen;
  - De interpretatie door stakeholders en het aansprakelijkheidsrisico.

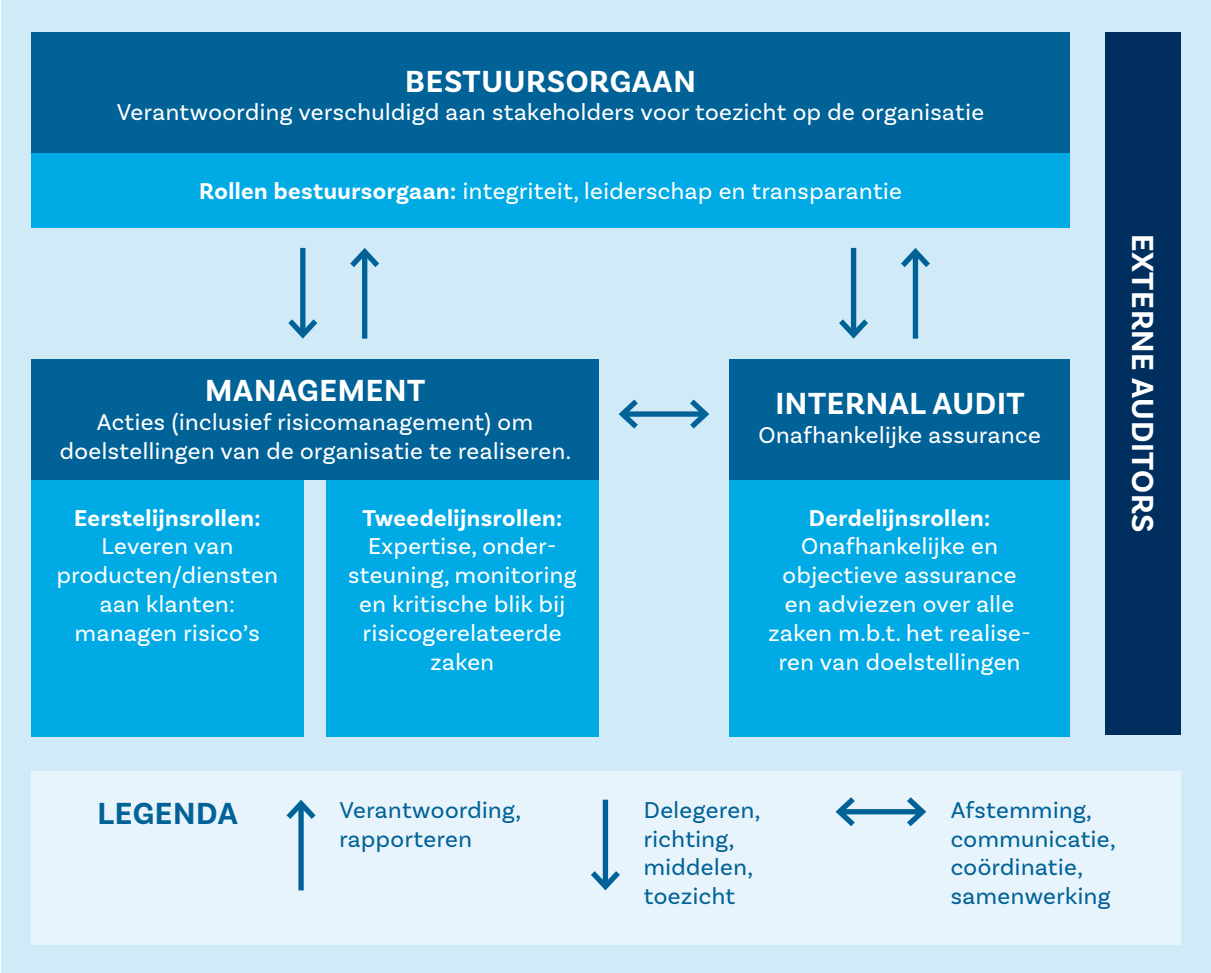
  Het zou kunnen helpen hierbij afstemming te zoeken met andere organisaties met een vergelijkbaar risicoprofiel, bijvoorbeeld per sector.
- Het **raamwerk** voor beheersing. De Code verwacht dat een raamwerk wordt gekozen en dat wordt aangegeven hoe het raamwerk in de beoordeling wordt toegepast. Expliciet noemt men het COSO-raamwerk voor interne beheersing als (enig) voorbeeld, maar de organisatie is vrij daarin andere keuzes te maken. Er zijn vele management control frameworks, met verschillen in nadruk op het steunen op beleid en procedures danwel de professionaliteit van medewerkers. De meeste organisaties zullen al gebruik maken van een dergelijk raamwerk. Het verdient aanbeveling aan te sluiten bij reeds gehanteerde raamwerken voor risicomanagement als geheel en voor de beheersing van specifieke risico's.

3 Wie moet wat doen?

Bij de VOR spelen alle actoren in de verantwoordingsketen een rol. Zeker als organisaties nog minder volwassen zijn in hun IRCS, is het belangrijk dat alle actoren nu met elkaar in gesprek gaan over de risico's van de organisatie en de beheersing daarvan.

3.1 Three lines-model als basis

IIA pleit daarbij voor het gebruik van het Three Lines-model. Dat model geeft aan dat het bestuursorgaan (te lezen als zowel de raad van bestuur als de auditcommissie) kan worden geïnformeerd vanuit 3 soorten functies, die elk een rol spelen bij risicobeheersing:



Figuur 1. Het Three Lines-model.

1. Het verantwoordelijke management, de 1e lijn, die primair verantwoordelijk is voor het identificeren en beheersen van risico's en de beoordeling van de effectieve werking van de risicobeheersing.
2. Daarbij ondersteund door 2e lijns gespecialiseerde functies (experts) als Risicomanagement, (Business) Control en Compliance, maar bijvoorbeeld ook door HRM voor personele risico's en de CISO voor cybersecurity-risico's. De 2e lijn ondersteunt het verantwoordelijke management met beleid, procedures en adviezen en met het monitoren van de naleving daarvan. Afhankelijk van de aard van de functie, kan zij ook onafhankelijk aan het bestuursorgaan rapporteren.
3. De IAF als 3e lijn, die onafhankelijk (van de 1e en 2e lijn) audits uitvoert en adviezen geeft over de opzet, werking en effectiviteit van de beheersing. De IAF beoordeelt of het geheel van de 1e en 2e lijn effectief is en kan verdiepende onderzoeken uitvoeren op specifieke thema's, processen en risico's.

Naast deze interne functies, zijn er de externe (4e lijns) assuranceproviders, zoals de externe accountant, maar mogelijk ook anderen, zoals een externe toezichthouder, een ISO-auditor of een visitatiecommissie die de kwaliteit van (de beheersing van) processen beoordelen.

Het model dient organisatie-specifiek te worden toegepast, en per risicogebied te worden afgestemd op de omvang en complexiteit van de risico's en op de risicobereidheid van de organisatie. Zeker voor kleine(re) organisaties zullen niet alle 3 genoemde lijnen van voor alle risico's noodzakelijk zijn of in aparte afdelingen dienen te worden georganiseerd. Buiten de financiële sector is, onder voorwaarden om de onafhankelijkheid te borgen, ook een combinatie van 2e en 3e lijns-taken mogelijk. De assurancemap, in 3.3 kan helpen hierin bewust de keuzes te maken.

3.2 De taakverdeling

Onderstaand overzicht toont de taken van de binnen de organisatie bij de VOR betrokken functies, en kan als vertrekpunt dienen om het 'systeem' te evalueren: **pakt iedereen haar rol?**

Bestuur	• Pakt de eindverantwoordelijkheid voor de VOR
	• Stelt (vooraf) vast dat het gehele systeem (IRCS) in opzet adequaat is:
	  • Alle materiële risico's zijn benoemd
	  • Daarop afgestemde beheersmaatregelen zijn gedefinieerd
	  • Verantwoording over opzet en werking van maatregelen en hun effectiviteit is georganiseerd
	  • Met 'aligned assurance': geen gaten, geen dubbel werk
	• Stemt dit af met de auditcommissie
	• Stelt vast dat gehele systeem (IRCS) ook werkt/effectief is
	• Stelt vast dat daarmee voldoende input voor de VOR is verkregen
	• Ondertekent de VOR

Auditcommissie	• Beoordeelt de wijze waarop de effectiviteit van de opzet en werking wordt, respectievelijk is beoordeeld • Beoordeelt de wijze waarop de VOR wordt respectievelijk is onderbouwd • Brengt verslag uit aan de raad van commissarissen
Raad van commissarissen	• Bespreekt het verslag van de auditcommissie en besluit in het kader van haar toezicht op de effectiviteit van de ICRS

1e lijn Management	• Informeert bestuur over:
	  • Realisatie van haar doelen
	  • De bijbehorende risico's en beheersing daarvan
	  • De beoordeling van de effectiviteit van de opzet en werking van de beheersing

2e lijn Risicomanagement	• Coördineert de opzet en uitvoering van het risicomanagement
	  • Met één 'taal' (risicoregister)
	  • Met één systematiek van risicomanagement en beoordeling van de effectiviteit daarvan
	  • Met op elkaar afgestemde taken – 'aligned assurance'
	• Ondersteunt (faciliteert) de uitvoering van het risicomanagement
	• Monitort de werking van de afspraken over het risicomanagement en informeert bestuur daarover

2e lijn Staven (Compliance, HR, IT, overig)	• Adviseert over beleid en procedures rondom specifieke bedrijfsaspecten (ofwel operationele en compliance risico's) • Ondersteunt (faciliteert) de toepassing door de 1e lijn • Monitort de werking van beleid en procedures en informeren bestuur daarover
3e lijn IAF	• Kan adviseren, als verbeteringen in het gehele systeem (IRCS) wenselijk zijn en de 2e lijns functie Risicomanagement dit niet al doet • Audit (risk based) de beheersing van belangrijke risicogebieden en totaliseert bevindingen waar mogelijk naar bedrijfsonderdeel, risicogebied of thema • Audit het risicomanagement van de organisatie, of meer specifiek het proces van het opstellen (onderbouwen) van de VOR • Inclusief de volledigheid en efficiency van de assuranceverlening • Toetst de concept-VOR op verenigbaarheid met bevindingen vanuit haar andere werkzaamheden
Externe accountant	• Toetst de concept-VOR op verenigbaarheid met bevindingen vanuit haar andere werkzaamheden, en op aanwezigheid en materiële afwijkingen

3.3 De assurancemap als nadere concretisering

Om de taken verder te concretiseren pleit het IIA voor zogenaamde 'integrated of aligned assurance', waarbij de taken en werkzaamheden van de drie lijnen én externe assurance-providers op elkaar zijn afgestemd, zodat wordt gewaarborgd dat alle materiële zaken worden opgepakt en er geen werkzaamheden dubbel worden gedaan. De IAF kan hierin een coördinerende rol spelen.

Assurancemapping is daarbij een belangrijk hulpmiddel, voor elk van de in 3.2 genoemde functies. Met een assurancemap wordt per doel of risico-(gebied) in kaart gebracht wie wat doet (respectievelijk zou moeten doen) en wat de huidige kwaliteit van die activiteiten is.

Het is aldus van essentieel belang dat de IAF de rollen en werkzaamheden afstemt met zowel bestuur en auditcommissie als met de andere interne en externe 'assurance-providers'.

Global Internal Audit Standards (GIAS) 9.5 Coördinatie en vertrouwen

Het hoofd van de internal auditfunctie moet samenwerken met interne en externe aanbieders van assurancediensten en afwegen of op hun werk kan worden vertrouwd. Coördinatie van dienstverlening beperkt het uitvoeren van dubbel werk tot een minimum , onderstreept lacunes in de dekking van de belangrijkste risico's en vergroot de algehele toegevoegde waarde van aanbieders.

	1e lijn							2e lijn					3e lijn	4e lijn		
	Operations	Marketing	Sales	...	Finance	Pers. zaken	ICT	Risk management	Business control	Compliance	CISO/Security	H&S	Internal audit	Externe accountant	ISO-auditor	...
Risicogebied																
Operationeel								■					■			
Marketing/verkoop		■	■					■					■		■	
Productkwaliteit	■							■				■	■			
Serviceverlening	■							■					■			
Cybersecurity	■	■	■	■	■	■	■	■			■		■			
HR	■	■	■	■	■	■		■					■			
Personeelbeheer	■	■	■	■	■	■	■	■					■			
								■					■			
Compliance								■		■			■			
Zorgplicht	■	■	■					■		■			■			
Wwft	■							■		■			■			
Privacy	■				■	■	■	■		■			■			
								■		■			■			
Financ. verslag								■	■				■	■		
					■			■	■				■	■		
					■			■	■				■	■		
Niet-financ. verslag								■	■				■	■		
					■			■	■				■	■		
					■			■	■				■	■		

Figuur 2. Assurancemap

4. Wat kan de IAF bijdragen?

4.1 De mogelijke rollen van de IAF

De rol van de IA in de governance wijzigt niet – deze blijft (bepaling 1.3) het beoordelen van de opzet en de werking van de IRCS. Dat sluit aan bij de doelstelling van IA, zoals vermeld in de nieuwe wereldwijde beroepsstandaarden van het IIA.

Internal auditing versterkt het vermogen van de organisatie om waarde te creëren, te beschermen en te behouden door het bestuur en het management te voorzien van onafhankelijke, op risico gebaseerde en objectieve assurance, advies, inzicht en vooruitzichten.
(Global Internal Audit Standards, 2024)

INTERNAL AUDIT:

- helpt de organisatie haar doelstellingen met succes te behalen
- versterkt de governance-, risicomanagement- en beheersprocessen van de organisatie
- verbetert de besluitvorming van en het toezicht op de organisatie
- versterkt de reputatie en geloofwaardigheid van de organisatie bij haar belanghebbenden
- vergroot het vermogen van de organisatie om het algemeen belang te dienen.

Allemaal elementen die direct danwel indirect ook worden beoogd met de VOR.

Hoewel de rol niet wijzigt, zullen de specifieke werkzaamheden wel wijzigen, doordat het bestuur nu een meer uitgebreide verklaring moet afgeven, en de auditcommissie deze, inclusief de onderbouwing, moet beoordelen.

Een IAF voert over het algemeen een combinatie van assurance- en adviesdiensten uit. In de IIA-standaarden zijn assurancediensten opdrachten waarin internal auditors objectieve beoordelingen uitvoeren om zekerheid (assurance[3]) te bieden.
Ook t.a.v. de VOR kunnen beide worden onderscheiden. Hierna wordt achtereenvolgens ingegaan op:

- assurance activiteiten;
- adviesactiviteiten gericht op het faciliteren van de onderbouwing van de VOR;
- adviezen gericht op de ‘implementatie’ van de VOR, ofwel over opzet en verbetering van de IRCS.

De voor de organisatie gewenste rol en diensten van de IAF zijn afhankelijk van de volwassenheid van de ‘three lines’ (met name van de 2e lijns-functies) en van de IRCS. In een organisatie waar deze systemen reeds goed functioneren en sprake is van een ‘volwassen’ 2e lijn, zullen de genoemde adviesactiviteiten vermoedelijk door de 2e lijn reeds zijn opgepakt. Dan kan de IAF volstaan met het geven van aanvullende zekerheid over die systemen.

3 Assurance wordt hierbij gedefinieerd als een verklaring bedoeld om het niveau van vertrouwen van belanghebbenden in de governance-, risicomanagement- en beheersprocessen van een organisatie met betrekking tot een kwestie, omstandigheid, onderwerp of beoordeelde activiteit te vergroten in vergelijking met vastgestelde criteria.

4.2 Assurance

Het beoordelen en geven van zekerheid over de kwaliteit van beheersing is zoals gezegd, één van de kerntaken van de IAF. Rapportages gaan zowel naar het bestuur als de auditcommissie (zie ook bepaling 1.3.5). Zij levert daarmee een belangrijke input voor de verklaring en voor het toezicht daarop.

4.2.1 AUDITS

Bij het geven van assurance door de IAF, kunnen de volgende onderzoeken worden onderscheiden:

1. Audits op de beheersing van specifieke risicogebieden;
2. Audits van het risicomanagement van de organisatie, mogelijk specifiek te richten op het proces van de onderbouwing van de VOR (wordt geborgd dat het bestuur over alle risico's een juiste en volledige verklaring op kan stellen?)
3. In organisaties met een minder volwassen IRCS kan worden overwogen een audit op de kwaliteit van de 2e lijns-functie uit te voeren. Figuur 3 toont een voorbeeld, waarin in de linkerkolom de kenmerken van een volwassen 2e lijnsfunctie staan en in de kolommen de diverse risicogebieden die worden ondersteund door de 2e lijnsfuncties.
4. Beoordeling van de concept-VOR, waarbij de IAF toetst of de VOR in overeenstemming is met de eisen uit de Code en met bevindingen van de IAF vanuit haar andere werkzaamheden.

Een effectieve en efficiënte combinatie van audits zou kunnen bestaan uit een jaarlijkse beoordeling van het VOR-proces en de concept-VOR, aangevuld met een roulerend geheel van audits op specifieke risicogebieden.

Deelvragen	Onderzoeksaspecten	Onderwerp A	Onderwerp B	Onderwerp C	Onderwerp D	Onderwerp E	Onderwerp F	Onderwerp G	Onderwerp H	Onderwerp I
A. Is de personele bezetting adequaat?	1. Functie aanwezig	G	G	G	G	G	G	G	G	G
	2. Bezetting	G	G	G	G	G	G	G	G	O
B. Is de faciliterende en adviserende rol adequaat?	1. Richtlijnen	O	N	O	O	O	G	O	N	R
	2. Advisering	G	N	O	R	O	G	O	N	O
	3. Facilitering	O	N	O	R	G	G	O	N	R
C. Is de monitoring rol adequaat?	1. Werkprogramma's	G	G	O	O	O	O	O	G	R
	2. Volledigheid	O	G	O	R	O	G	O	G	R
	3. Vastlegging	G	O	G	O	G	O	O	G	R
	4. Efficiency	G	G	G	R	O	G	O	G	R
D. Wordt er geleerd vanuit de 2e lijn controles?	1. Rapportage	G	N	O	R	G	O	G	N	R
	2. Verbetering	O	N	O	R	G	O	G	N	R

Groen (G)	(vrijwel) aan alle criteria is voldaan
Oranje (O)	niet aan alle criteria is voldaan → op sommige punten wordt risico gelopen, maar samenvattend is er geen ernstige situatie
Rood (R)	aan een groot aantal of belangrijke criteria wordt niet voldaan → er is sprake van een groot risico voor het bereiken van de doelen

Figuur 3. Audit op kwaliteit van de 2e lijnsfuncties.

4.2.2 RANDVOORWAARDEN

Belangrijke 'technische' randvoorwaarden om de assurance rol goed te vervullen zijn:

- Een voor de gehele organisatie gezamenlijk risicoregister, afgestemd op de strategische doelen van de organisatie. Van de IAF wordt een eigen inschatting van de risico's verwacht; de in te schatten risico's dienen echter hetzelfde te zijn om verwarring te voorkomen en te zorgen dat de verschillende assurance-providers niet langs elkaar heen werken. Dit risicoregister vormt de basis voor de assurancemap.
- Een gezamenlijke materialiteitsanalyse, waarmee wordt bepaald welke risico's echt van materieel belang zijn voor de organisatie en aan de basis staan van het risk-based auditplan van de IAF.

  De vanuit CRSD verplichte 'dubbele materialiteitsanalyse' kan hier als extra input voor worden gebruikt c.q. dient hiermee in lijn te zijn.
- Een indeling van de audituniverse, die aansluit bij de materialiteitsanalyse.

  Met de audituniverse wordt de organisatie als het ware ingedeeld in 'auditbare brokken'. Vanuit de onderscheiden risicogebieden kan het zijn dat deze universe naar verschillende invalshoeken dient te worden ingedeeld, bijvoorbeeld naar organisatorische eenheden, naar wetgeving, naar specifieke risicogebieden of naar thema's. Ook bij deze indeling is belangrijk voor ogen te houden vanuit welke optiek het bestuur de VOR wil opstellen?
- De vertaling van de audituniverse naar het auditplan, waarmee de audits en frequentie daarvan worden vastgesteld. Dat leidt tot een risk-based auditplan. Daarbij zullen niet alle relevante risico's jaarlijks door de IAF worden beoordeeld; daarvoor is de capaciteit onvoldoende, maar dat is ook niet nodig gegeven de werkzaamheden van de 1e en 2e lijn. Die zijn continue en worden dan aangevuld met onafhankelijke, roulerende, audits, zodat bijvoorbeeld in een 4-jaarscyclus alle significante risicogebieden door de IAF worden geaudit.

  De IAF dient daarbij te beoordelen of de afdekking van de audituniverse voldoende is c.q. dat voldoende audits kunnen worden uitgevoerd om de van de IAF verwachte rapportages te kunnen opleveren. Ook achteraf dient de IAF vast te stellen dat de afdekking inderdaad voldoende is geweest en dat er voldoende onderbouwing aanwezig is voor de van de IAF gevraagde conclusies.

  Tenslotte speelt hier de diepgang van de audit een rol. Welke mate van zekerheid dient in welke rapportage te worden gegeven. Is bijvoorbeeld een positieve conclusie ('vastgesteld is dat …') vereist, of kan volstaan worden met een minder diepgaande analyse en een negatieve conclusie ('er is niet vastgesteld dat het niet goed gaat').
- Rapportage per audit en overkoepelend. Het geheel van auditwerkzaamheden leidt gebruikelijk tot rapportages per audit en samenvattende rapportages naar een overkoepeld geheel (zoals een bedrijfsonderdeel, thema of specifiek risico). Zo zou vanuit rapportages per proces een overall conclusie per bedrijfsonderdeel of per wet worden getrokken.

  Om te kunnen dienen als onderbouwing van de VOR is het belangrijk, en ook geëxpliciteerd in de IIA-beroepsstandaarden, dat de conclusie daarbij een oordeel geeft over de ***effectiviteit*** van de beheersing. Volstaan met het alleen beschrijven van omissies in opzet en/of werking van de te verwachten beheersmaatregelen is onvoldoende; deze omissies dienen in het kader van de risicobereidheid en de (kans op) realisatie van de doelen te worden geplaatst.[4]

4 Het begrip effectiviteit wordt in praktijk verschillend uitgelegd. Vaak bedoelen auditors hiermee de vaststelling dat beheersmaatregelen 'werken' in de praktijk. Dat is echter nog niet de vraag of daarmee (wordt geborgd dat) de doelen worden behaald. Vergelijk het verschil tussen de aanwezigheid van waarschuwingsbordjes bij een natte vloer en de vraag of er (toch) mensen uitglijden. De Code laat dit open, om door de organisatie zelf te worden ingevuld.

- De planning van de rapportages, met name van de samenvattende rapportages in aanvulling op de individuele audits, bijvoorbeeld per kwartaal om tijdig als basis voor de VOR te kunnen dienen.

Zoals gezegd kan de IAF naast de uitvoering van audits de organisatie ook met adviesdiensten in het kader van de VOR ondersteunen, zowel in de uitvoering ofwel onderbouwing van de VOR, als in de implementatie van de VOR, ofwel benodigde verbeteringen van de IRCS. Daarop wordt in de volgende paragrafen nader ingegaan.

4.3 Advies gericht op de onderbouwing van de VOR

In de uitvoering van het risicomanagement, ter onderbouwing van de VOR, kan de IAF, passend bij haar kerntaken en volgend uit haar brede kennis van de organisatie en helicopterview:

- optreden als 'coördinator' tussen de diverse (in- en externe) assurance providers, op basis van de assurancemap (zie 3.2.1.);
- de voortgang en realisatie van het geheel (van de onderbouwing) bewaken;
- in overleg met bestuur en auditcommissie, beoordelen of er externe of interne ontwikkelingen zijn, die leiden tot wijzigingen in risico's, die tot een aanpassingen van de plannen zouden moeten leiden;
- helpen bij het identificeren van tekortkomingen in de beheersing, maar ook adviseren hoe deze te verhelpen en vervolgbeoordelingen uitvoeren om te bepalen of deze adequaat zijn aangepakt;
- reflecteren op de conceptverklaring, met name of deze aansluit bij de onderliggende bewijsvoering.

4.4 Advies gericht op de implementatie van de VOR

De aansturing van de implementatie van de VOR is in beginsel een 2e lijns-rol. Met name Risicomanagement lijkt daarvoor de passende functie. Tegelijkertijd zien we, net als bijvoorbeeld destijds bij de implementatie van SOx, dat de 2e lijn niet altijd voldoende bemenst is en de IAF deze rol (tijdelijk) oppakt.

Belangrijke elementen bij de implementatie, waarop de IAF zou kunnen adviseren, zijn:

- de uitwerking van de rollen van de diverse betrokken (1e en 2e en 3e lijns-)functies voor de 4 onderscheiden risico-categorieën, met behulp van een assurancemap, om te komen tot 'aligned assurance' en daarmee een zowel effectieve als efficiënte aanpak (zie ook 3.21.);
- de opzet en uitvoering van de materialiteitsanalyse van de risico's op alle vier de risicocategorieën;
- de wijze van het (door de 1e lijn) definiëren van de risk appetite ofwel risicobereidheid op de diverse materiële risico's;
- de raamwerken voor risicobeheersing (die, gegeven het belang daarvan voor de goede werking, ook aandacht voor cultuur en gedrag in zich zouden moeten hebben);
- de training van het management in risico bewustzijn en -beheersing, om eigenaarschap en een goede inbedding te waarborgen;
- de invulling van de 'onderbouwing' van de VOR (temeer van belang daar expliciet aan de auditcommissie de opdracht is meegegeven de wijze van onderbouwing te beoordelen).
  Overwogen kan worden het verantwoordelijke management voor de diverse functies en risico's een interne VOR of 'LOR' (Letter of Representation) af te laten geven; ook dan dient bepaald te worden hoe deze dient te worden gesubstantieerd;

- good practices in de opzet van toetsactiviteiten door de 1e en 2e lijn; en documentatie daarvan;
- de tekst van de verklaring[5], met specifieke aandacht voor de betekenis en mogelijke rating van de (positieve of negatieve) 'zekerheid' over de beheersing van de operationele en compliance risico's en van 'tekortkomingen'.

Samenvattend

Het kunnen beantwoorden van de vraag van de CEO 'of hij mag tekenen', of van de vraag van de voorzitter van de auditcommissie 'of de VOR klopt', is niet simpel met een ja of nee te beantwoorden en vereist een zorgvuldige opzet van de IRCS en de activiteiten van de IAF in samenhang met de activiteiten van de 1e en 2e lijnsactiviteiten, én uitvoering daarvan.

De IAF kan bestuurders en commissarissen een belangrijk deel van de oplossing bieden voor de uitdagingen die de nieuwe VOR kan bieden, als assurance provider en als problem solver of adviseur.

- In de nieuwe Code worden middels de VOR aanvullende eisen aan het bestuur (en auditcommissie) gesteld, met name ten aanzien van de verantwoording over:
  - De effectiviteit van de risicobeheersing;
  - Operationele en compliance risico's.
- Deze eisen zullen de aandacht voor risicomanagement en beheersing vergroten en daarmee van waarde zijn voor de organisatie en haar belanghebbenden.
- Deze eisen kunnen, gegeven de complexiteit en verscheidenheid van deze risico's, afhankelijk van de volwassenheid van haar IRCS, uitdagend zijn voor het bestuur.
- De IAF is specialist op het gebied van (het onafhankelijk beoordelen) van de governance, risicomanagement en beheersing van de organisatie, en kan op basis van die positie, vaardigheden en verkregen kennis het bestuur en de auditcommissie met audits en advies ondersteunen bij de VOR.
- De IAF zal in haar audits echter niet (jaarlijks) alle relevante risico's afdekken; input (onderbouwing) van de VOR wordt verkregen vanuit het samenspel van 1e, 2e en 3e lijn.
- Hiertoe dienen tussen het bestuur en de IAF duidelijke afspraken te worden gemaakt over:
  - De rol van de IAF, gerelateerd aan de audit universe, en de afstemming met 1e en 2e lijn;
  - Het jaarplan, de afdekking van de audituniverse in het boekjaar en de gewenste rapportages.
- Het maken van dergelijke afspraken is tegelijkertijd een van de vereisten voor de implementatie van de nieuwe beroepsstandaarden van internal audit (GIAS).

5 In de toelichting bij de wijziging van de Code is daarbij aangegeven:
- *'zekerheid' is NIET 'assurance' als in accountancy;*
- *'effectiviteit' is NIET 'effectivity 'zoals in SOX.*

Bijlage 1. Duiding van de wijzigingen in de huidige Code

Onderstaande tabel geeft aan wat er in de huidige Code is opgenomen over de VOR en wat daaraan middels het voorstel van de schragende partijen en NBA wordt gewijzigd.

NIET gewijzigd	Nieuw in voorstel schragende partijen en NBA
1.2 Risicobeheersing Bestuur verantwoordelijk voor identificeren en beheersen risico's • 1.2.1 Inventariseren en analyseren (strategische, operationele, compliance en verslaggevings) risico's • 1.2.2 Implementatie interne risicobeheersings- en controlesystemen (IRCS) • 1.2.3 Monitoring opzet en werking (O&W)	Geen wijzigingen.
1.4 Verantwoording over risicobeheersing Bestuur legt verantwoording af over effectiviteit van de O&W van IRCS • 1.4.1 bestuur bespreekt effectiviteit van de O&W IRCS met AC en legt daarover verantwoording af aan RvC • 1.4.2 Verantwoording in bestuursverslag over i. Uitvoering risicoanalyse + beschrijving voornaamste risico's ii. O&W IRCS afgelopen boekjaar iv. Tekortkomingen, significante wijzigingen v. Gevoeligheden in de resultaten voor materiële wijzigingen in externe omstandigheden	*Verantwoording is verbreed:* *- + verantwoording over beoordeling effectiviteit* *- echter exclusief strategische risico's* ii + O&W op gebied van **operationele, compliance en verslaggevingsrisico's** (+raamwerken) *– dus excl. strategische risico's* iii **+ beoordeling effectiviteit** van de IRCS m.b.t. operationele, compliance en verslaggevingsrisico's
• 1.4.3 Verklaring van het bestuur: i. Verslag geeft inzicht in tekortkomingen in werking IRCS ii. De ICRS geeft redelijke mate van zekerheid over financiële verslaglegging v. Financiële verslag o.b.v. going concern vi. Materiële risico's vermeld	*Verklaring is verbreed* iii **+ beperkte mate van zekerheid over duurzaamheidsverslaglegging** iv **+ welk niveau van zekerheid** IRCS geven dat **operationele + compliance** risico's **effectief** worden beheerst - *dus niveau van zekerheid zelf te definiëren*
• 1.5.3 Verslag auditcommissie	*Rol auditcommissie verbreed* iv. … en de wijze waarop de verklaring zoals bedoeld in 1.4.3 is onderbouwd

Tabel 1. Wat is er wel / niet gewijzigd ?

Ten aanzien van de verklaring van het bestuur vallen drie zaken op:

1. Strategische risico's: deze maken deel uit van de risicobeoordeling (2.1) en de beschrijving van de voor de organisatie belangrijkste risico's (1.4.2 sub i), maar behoeven niet geadresseerd te worden in de beschrijving van de opzet en werking en van de beoordeling van de effectiviteit (1.4.2 sub ii en iii) noch te worden opgenomen in de bestuursverklaring zelf (1.4.3).[6]
2. Het is belangrijk onderscheid te maken tussen de gevraagde verantwoording en verklaring: De verantwoording vraagt om een **beschrijving** van de opzet en werking respectievelijk (en dat is nieuw) van de beoordeling van de effectiviteit. Dat is echter nog geen **verklaring** dat de IRCS inderdaad effectief zijn ofwel verklaring van het resultaat, in termen van de zekerheid die deze IRCS bieden. Dat laatste wordt wel vereist in de verklaring (1.4.3).

Soort risico	Opzet en werking	Beoordeling effectiviteit	Verklaring mate van zekerheid
	beschrijving	beschrijving	conclusie

3. In 1.4.3 wordt ten aanzien van de operationele en compliance risico's in de toelichting aangegeven dat het bestuur zelf aangeeft "welk niveau van zekerheid de systemen geven dat de operationele en compliance risico's effectief worden beheerst". Daarbij wordt aangegeven dat het woord 'zekerheid' in dit verband niet moet worden gelezen als het in de accountancy gehanteerde begrip 'assurance', noch is bedoeld dat ondernemingen hiervoor een vast kader moeten hanteren. Evenmin wordt met 'effectiviteit' aansluiting gezocht bij het gelijkluidende begrip uit de Amerikaanse wetgeving (i.c. de Sarbanes-Oxley wet (SOx)). Nadrukkelijk wordt daarbij aangegeven dat het mogelijk is aan te geven dat bepaalde risico's naar hun aard niet effectief kunnen worden beheerst, of dat de effectiviteit van voornoemde systemen niet kan worden vastgesteld.[7] Deze definitie wordt dus aan de organisatie zelf overgelaten, "mede in het licht van de risicobereidheid van de organisatie".
   Dit vormt een uitdaging, ook om begripsverwarring bij stakeholders te voorkomen. Tegelijkertijd is dit een mooie oplossing. Eerder was in de 'Code Tabaksblat' een brede VOR opgenomen, maar dat bleek vaktechnisch en juridisch moeilijk haalbaar: kun je überhaupt een In Control Statement (ICS) afgeven en kan dit op alle gebieden met een redelijke mate van zekerheid en welke juridische risico's loop je daar als bestuurder mee? We zien nu dat de schragende partijen en NBA, ook vanuit een sterke maatschappelijk druk, een 'oplossing' hebben gevonden, door voor de te onderscheiden risicogebieden een verschillende maten van zekerheid te verwachten.

6 In de toelichting wordt daarover gezegd: *Ter zake strategische risico's kan een onderscheid worden gemaakt tussen de besluitvorming over de strategie en de implementatie ervan. De risicobeheersingssystemen zien niet toe op de besluitvorming over de strategie. Risico's die samenhangen met de implementatie van de strategie vertalen zich in operationele, compliance en verslaggevingsrisico's. Zonder afbreuk te doen aan de benodigde robuustheid van de strategiebepaling geldt dat veel strategische risico's niet voor risicobeheersing vatbaar zijn omdat zij geheel of ten dele buiten de invloedsfeer van de vennootschap liggen.*
Als IIA menen we dat strategische risico's, hoewel vaak buiten de directe invloedssfeer van de organisatie, wel degelijk vatbaar zijn voor risicobeheersing, en dat het ook belangrijk en veelal gebruik is om bij en na het nemen van strategische beslissingen zowel de kansen als bedreigingen in beeld te brengen en te bewaken.

7 In de toelichting wordt als voorbeeld gegeven: "de naleving van wet- en regelgeving, waarbij de vennootschap mede afhankelijk is van het gedrag van haar medewerkers wereldwijd, terwijl hun gedrag niet redelijkerwijs voortdurend beheerst kan worden of volledig in procedures kan worden verankerd".

Bijlage 2. De actoren en hun rol

De volgende actoren kunnen worden onderscheiden:

Actor	Rol
Bestuur	Opstellen VOR
Auditcommissie – RvC	Beoordelen VOR en haar onderbouwing
Management	Leveren input voor de verklaring
Staven, als Risicomanagement, Compliance, Legal, overige	
IAF	
Externe accountant	Beoordelen verenigbaarheid met jaarrekening(controle)

Bestuur en Auditcommissie

In de Code zelf wordt naast de taak van het bestuur alleen de rol van de auditcommissie (AC) aangepast. Logischerwijs dient zij de nieuwe elementen in het bestuursverslag te beoordelen. Daarbij wordt expliciet aangegeven dat zij ook over de wijze waarop de VOR is onderbouwd, dient te rapporteren aan de raad van commissarissen (RvC). De onderbouwing dienst dus zodanig te zijn dat de AC er comfortabel mee is.

IAF

De rol van de internal auditor (1.3) wijzigt niet in de Code, maar de werkzaamheden zullen door de invoering van de VOR wel veranderen. Volgens de Code heeft de IAF als taak (onafhankelijk) de opzet en de werking van de IRCS te beoordelen. Met de nieuwe VOR wordt de rol van de IAF des te belangrijker. Naast de verklaring over de financiële verslaggeving, die al in de Code was opgenomen, dient nu ook aandacht te worden besteed aan de duurzaamheids-verslaggeving en aan de beheersing van operationele en compliance risico's. Deze risico's vormen traditioneel al een belangrijk object van internal audits.

Externe accountant

Ook de rol van de externe accountant (1.7) wijzigt niet; maar ook hier geldt dat de werkzaamheden door de VOR wel veranderen. De VOR is immers onderdeel van het bestuursverslag, dat door de accountant wordt beoordeeld in de jaarrekeningcontrole. Daarbij wordt getoetst op verenigbaarheid met de jaarrekening en met wat tijdens die controle is waargenomen (verenigbaarheidstoets, aanwezigheidstoets en signaleren van materiële afwijkingen)[8].

De kennis van de externe accountant over de IRCS kan per gecontroleerde organisatie verschillen. Dat is mede afhankelijk van de keuze van de mix van systeem- en gegevensgerichte controlewerkzaamheden. Een keuze die op haar beurt mede afhankelijk is van de mate van robuustheid en volwassenheid van de IRCS. Voor de rol van de externe accountant wordt verder verwezen naar de Dialoogpaper van het NBA.

Three Lines

Het bestuur zal zich bij het opstellen van de VOR baseren op de input vanuit de IAF, maar ook, en eigenlijk primair, op input vanuit het verantwoordelijke management en de staven die zich met risicobeheersing bezig houden, zoals Risicomanagement, (Business) Control en Compliance. Het is zaak de rollen en inbreng goed op elkaar af stemmen, om zo op effectieve en efficiënte wijze tot een VOR te komen. De IAF kan hierbij een faciliterende rol spelen.

8 NBA zal daartoe haar Handreiking 1109 'Accountant en corporate governance informatie' aanpassen.

Instituut van
Internal Auditors
Nederland