Grant Thornton

An instinct for growth™

Grote twijfel of risicomanagement voldoende is geactualiseerd?

Commissarissen benchmarkonderzoek risicomanagement 2019-2020

Door:
Aalt Klaassen
Dirk-Jaap Klaassen
Oscar Toebosch
Herbert Rijken

Grote twijfel of risicomanagement voldoende is geactualiseerd

Commissarissen benchmarkonderzoek risicomanagement 2019-2020

door:
Aalt Klaassen
Dirk-Jaap Klaassen
Oscar Toebosch
en
Herbert Rijken

Grote twijfel of risicomanagement voldoende is geactualiseerd?

Waarom deze titel?

- Uit het onderzoek blijkt grosso modo dat de respondenten doorgaans vinden dat er door de rvc voldoende aandacht wordt besteed aan risicomanagement.
- Bij de vraag of er voor een aantal met name genoemde calamiteiten/risicogebieden draaiboeken zijn of moeten zijn, is de hoofdconclusie dat deze er voor nagenoeg alle genoemde gebieden beslist moeten zijn. Dat is de wenselijke situatie. De praktijk voor de meeste onderzochte risico's is dat deze er niet in de gewenste mate zijn of soms zelfs afwezig. Maar tijdens de interviews bleek ook dat menig respondent, zowel commissaris, bestuurder als secretaris of internal auditor geregeld veronderstelde dat er een draaiboek was. Maar niet wisten hoe het stond met de actualiteit ervan. Ergo de vraag is of de aandacht voor risicomanagement niet primair een 'papieren' exercitie is.
- Op grond van de uitkomsten van het belang van bepaalde risico's bij de afzonderlijke benchmarks vragen wij ons af of de commissarissen, maar ook de bestuurders en internal auditors, wel voldoende open minded naar risico's en risico-management kijken. We kunnen ons niet aan de indruk onttrekken dat bedrijfs- en sectorblindheid in combinatie met onvoldoende toekomstgericht kijken en onvoldoende 'zelf-denken' (dus niet zomaar de opvattingen van de buurman of de rvb overnemen) sommige risico's ten onrechte bagatelliseren. Het betreft zowel de kans van voorkomen als ook de (mogelijke) gevolgen van het optreden van een risico.

Over de auteurs

Aalt Klaassen
Researcher/consultant, partner bij Board in Balance bv en zelfstandig bestuursadviseur. Ruim 45 jaar werkervaring, onder andere in ondernemingsfinanciering, investor relations, (kapitaal)marktonderzoek, management development en good governance. Voormalig partner Rematch bv en voormalig medewerker Ondernemingsfinanciering aan de Economische faculteit van de Vrije Universiteit te Amsterdam. Aalt is bedrijfseconoom.

Dirk-Jaap Klaassen
Researcher/consultant en partner bij Board in Balance bv. Sinds 2008 verbonden aan Aalt Klaassen bv. De afgelopen jaren heeft hij diverse evaluaties (mede)begeleid en meegewerkt aan het jaarlijkse commissarissen benchmarkonderzoek. Dirk-Jaap is historicus.

Oscar Toebosch
Researcher/consultant, partner bij Board in Balance bv en zelfstandig bestuursadviseur met specialisaties governance, strategie (businessplannen, performance management) en verantwoording (integrated reporting). Hiervoor (tot 2012) circa 20 jaar werkervaring in marketing, communicatie en investor relations (vastgoed, woningmarkt, industrie/bouwsector). Oscar heeft een MBA van Vlerick Business School / KU Leuven.

Board in Balance is een onafhankelijke organisatie die evaluaties van raden van commissarissen en raden van toezicht uitvoert en onderzoek verricht naar governance.

Herbert Rijken
Hoogleraar Ondernemingsfinanciering aan de School of Business and Economics van de Vrije Universiteit te Amsterdam. Herbert heeft gestudeerd aan de Technische Universiteit Delft en de Universiteit Nyenrode, heeft promotieonderzoek uitgevoerd in de toegepaste kernfysica aan de Technische Universiteit Eindhoven en is werkzaam geweest als adviseur ondernemingsstrategie en bestuur. Zijn huidige onderzoek richt zich voornamelijk op kredietrisico, structured finance, financieringskosten en besturingsvraagstukken in ondernemingen.

Inhoud

Leeswijzer

Belangrijkste bevindingen, discussievragen en inleiding

In het **begin van** het **rapport** zijn de belangrijkste bevindingen en een aantal **discussievragen** gegeven. Hierna volgt een inleidend hoofdstuk met een korte achtergrond van het rapport en verantwoording van het onderliggende onderzoek. Resultaten worden gepresenteerd voor een gekozen **basisprofiel** van een commissaris en **zeventien profielen** (ook wel **benchmarks** genoemd)[1].

Margeteksten

In de **marges** worden de telkens volgens de auteurs meest kenmerkende punten neergezet. U kunt desgewenst door de margetekst scrollen om een beeld te krijgen van de belangrijkste punten. En wilt u wat meer weten, dan kunt u naar de bijbehorende tekst gaan.

Bespiegelingen/ vragen

Meestal aan het eind van elke paragraaf is een onderdeel opgenomen **'bespiegelingen/ vragen/ kanttekeningen'**. Deze dragen een onderzoek overschrijdend karakter. En geven soms de persoonlijke mening van de auteurs weer. Ze hebben tot doel commissarissen te stimuleren om al dan niet met de volledige rvc eens dieper op bepaalde onderwerpen in te gaan.

Onderwerpen en verbijzondering resultaten

Aan de orde komen: het **belang** van **risico's**, de wenselijkheid van **uitspraken** door de **internal auditor** en/of de **externe accountant** over deze risico's en de huidige en wenselijke situatie ten aanzien van de aanwezigheid van **draaiboeken** voor bepaalde risico's/ calamiteiten. Per paragraaf wordt eerst een **figuur met resultaten** neergezet. Daarbij zijn steeds de resultaten voor het **basisprofiel (= bapr)** opgenomen. Na de bespreking van de resultaten van het basisprofiel wordt gewezen op grote, belangrijke en opvallende afwijkingen bij de zeventien andere profielen/benchmarks.

Gehanteerde schaal

Bij de **gesloten vragen** is gebruik gemaakt van een **5-puntsschaal** met onder andere 1 = volstrekt oneens /zeer onbelangrijk tot 5 = volstrekt mee eens/zeer belangrijk.

Quotiënt als indicatie veranderwens. Klassen veranderwensen:
- acceptabel
- fors en
- urgent

Op basis van de scores voor de huidige en de gewenste situaties worden veranderwensen berekend. Als een indicatie voor een **veranderwens** worden quotiënten gebruikt. De gemiddelde score voor de **'huidige situatie'** is **gedeeld** door de gemiddelde score voor **'wenselijke situatie'.** Een waarde van 1.0 duidt op een evenwicht tussen de bestaande situatie en de geambieerde positie. Een waarde van 0.81 geeft aan dat de score voor 'de huidige positie' in negatieve zin 19 procent afwijkt van 'de gewenste positie'. Verandering is dan nodig. Het **quotiënt** is een **indicatie** van de **mismatch** tussen **wenselijke** en huidige positie en geeft de ambitie van de respondenten weer in termen van gewenste veranderingen (quotiënt < 1.0) of juist een temporisering van de ambitie (quotiënt > 1.0).
Een **afwijking** van maximaal **tien procent** naar beneden of naar boven (score vanaf 0.9 tot 1.1) wordt in dit rapport als **acceptabel** beschouwd. Een **negatieve afwijking** tussen de **tien** en **twintig procent** noemen wij een **forse veranderwens**. Negatieve afwijkingen **boven** de **twintig** procent duiden op een **zeer ongewenste** situatie en wordt omschreven als een **urgente veranderwens**.

Bespreekbaar punt en verbeterwens

De **veranderwensen** worden opgedeeld in **verbeterwensen** (ambitieniveau is dan ≥ 3.2) en **bespreekbaar geworden** punten (ambitieniveau < 3.2). Deze laatste categorie blijkt in de loop der tijd geregeld te migreren naar een verbeterwens, omdat de ambitie hoger komt te liggen.

1 De term basisprofiel en benchmarks naast het basisprofiel zijn toegelicht in paragraaf 1.2.

Verander-/verbeterpercentage als indicatie van mate van gedeelde verbeterwensen

Bij de veranderwensen wordt ook de term **verander-/verbeterpercentage** gehanteerd. Dit is het totaal aantal verander-/verbeterwensen als percentage van het totaal aantal mogelijke opties. Zo wordt er gewerkt met een verbeterpercentage van de bedrijfsprofielen (inclusief basisprofiel), van de persoonsgebonden profielen en van de niet-commissaris groep 'directie/secretaris gezamenlijk'. Het verander-/verbeterpercentage is een indicatie van de mate waarin op een bepaald onderdeel de verander-/verbeterwensen wel of niet breed worden gedeeld.
Na de verbeterwensen worden geregeld nog opmerkingen gewijd aan de huidige situatie.

Benchmarks/profielen verdeeld in bedrijfsprofielen en persoonsgebonden profielen.

In de tabel met de quotiënten zijn de resultaten gegeven voor het **basisprofiel** (bapr) en zeven variaties/benchmarks. Deze betreffen: **MKB**: het mkb bedrijf; **Corp**: de woningcorporatie; **Zorg**: bedrijf/instelling in de zorg- en welzijnssector; **VZ**: de voorzitter van de raad van commissarissen of raad van toezicht; **VR**: de vrouwelijke commissaris; **DIR**: lid van een rvb/directie die als bestuurder heeft ingevuld en **IA**: internal auditor. Voor de overige profielen zie tabel 1.

bapr

basisprofiel

MKB

commissaris bij een MKB-bedrijf

Corp

woningcorporatie

Zorg

bedrijf/instelling in de zorg- en welzijnssector

VZ

voorzitter van de Raad van Commissarissen of Raad van Toezicht

VR

vrouwelijke commissaris

DIR

lid van een rvb/directie die als bestuurder heeft ingevuld

IA

internal auditor

Daarnaast is er een kolom '**totaal**' opgenomen met het totaal aantal veranderwensen van alle profielen voor het betrokken aandachtpunt/de stelling.
De profielen zijn onderscheiden in **bedrijfsprofielen** (bapr, GB, MKB, Fam, Corp, Zorg, OW, ONP en 1tier), **persoonsgebonden profielen** (VZ, RvB, Jong, VR en AC) en **niet-commissaris** (DIR, Secr en IA).

Commissarissen, bestuurders, secretarissen en internal auditors die hun medewerking hebben verleend[2]

S. Addink-Berendsen
G.A. Anbeek
V.D. van Baasbank
R.L. de Bakker
P. Bennemeer
J. Benschop
M. Blom
M.K.H. Bode
M.A. Bongers
C.A.M. de Boo
G. Boon
C.H. van den Bos
R. Bosveld
T. Bruijninckx
A. van der Burg
B.I. van der Burg
W.A.P.J. Caderius van Veen
F. Candel
E. Capitain
F.J.H. Carstens
W.G.F. Cassée
G. Citroen
J.B. Crol
S. Croonenberg
A.F.A.A. Cuijpers
D.J.N.M. Curfs
E. Dannenberg
F.B. Deiters
T.R. Doesburg
H.W. van Dorp
G.A.C. van Dorst
R. Eijsvogel
A. Elsenaar
R.M. van Erp-Bruinsma
G. van Essen
F. Eusman
R. Florijn
J. Gardenbroek
E.J. van Garderen
E. Geerdink
M.C. van Gelder
J.J.K. Gerards
L.M. van der Goes
E.J.C.M. Gieben
F. Gommer
R.A.M.M. Gradus
J.R.J. Greitemann
A.F. Groen
J.V. Groenendijk
D. Haank
W.H.C.M. Hamers
C.J. Hartog
T.J.L.M. van der Heijden
J. Heikoop
J. Heimel
M.H. Hendrikse
F.A.M. van den Heuvel
F.N.M. van Heyningen
L.J.M. Hobert
P.G.M. Hofsté
J. Hol
A.E. Hol
Y.F.W. Hoogtanders
J.C. Hordijk
J.C. van Houwelingen
H. ten Hove
R.S. Icke
M.C. van der Jagt
P.J. de Jong
J. de Jong
B. Jonker
M.A.J. Keita
F.A.M. Keurentjes
F.W.M. Kevenaar
T. Kloet
J. de Kok
J. de Kreij
R.C. Kriekaard
A. Lambert
B. Lanza
C.A.M. Laurant
P.W. van Lingen
J.C. Lobbezoo
J.J. van Loon
W.A.J. van Loon
P.G. Luscuere
A. Man
E.A. Marseille
H. Maters
J.E.C. Müller
M. Muller
J.T.M. Munten
P. Nabuurs
J.J. Nooitgedagt
H.L.J. Noy
L. Nugteren
E. Obbink
D.P.C. Ochtman
M.H.J. Oomes
H.S.M. van Oostrom
S.V. Orlova
G.G.H. Peters-Meijers
J. Ploeg
K. van de Poppe
M. van Riel
C.J.M. van Rijn
J.P. Rijsdijk
F.A. van Rooij
J.P. van Rossum
R.J. Routs
A.N.G. Ruis
P.A.M. Sampers
J.C.M. Sap
F. Schellekens
E.J.J. Schenk
L.B.J. Schmitz
J.C.M. Schönfeld
M.J.C. Schoordijk
F.H.W. Schrijer
R. Sijberden
R. Smith
K.J.H.M. van Sleeuwen
E. Smeets
T.E. Smits-Hoekstra
H. Snijders
M. Sombroek
J.L. Spaan
H.C. Spoon
J. van der Starre
R. van der Steeg
J. Straathof
M. Stroop
D.M. Swagerman
T.G. Tiessen
S. Timmerman
M. Trompetter
L.J. Urlings
A.P.M. van der Veer
D.G. Vierstra
E.C.J.M. van der Voorn
P. van der Voort
R. de Vos
J.C.J. Vulto
C.W. van der Waaij
T. de Waard
L. Walraven
B.G.J.T. Wein
P. Westenberg
K.G. Westhoff
A.J.A. Wiechmann
M.P. van de Wiel
C. de Witte
T.M. de Witte
H.G. Wokke
T. Yousif
H.H.J. Zegering Hadders
A. Zegers-Bankert
T.R. Zomer
D. Zwaveling

2 Opgenomen zijn de namen van commissarissen, bestuurders, secretarissen en internal auditors die daarvoor toestemming hebben gegeven.

Voorwoord van Björn Roskott

Voor u ligt het rapport 'risicomanagement' van het commissarissenbenchmarkonderzoek 2019-2020. Het is de elfde editie waarbij Board in Balance, Herbert Rijken en Grant Thornton de krachten bundelen om een bijdrage te leveren aan het professionaliseren van de commissariaat in Nederland.

Risicomanagement is niet nieuw. Het is sinds mensenheugenis onderdeel van ons bestaan en is in elke onderneming aanwezig. Echter niet in elke organisatie is risicomanagement expliciet onderdeel van de strategie en cultuur.

Vandaag de dag veranderen de omstandigheden waarin een onderneming opereert sneller dan ooit. In een maatschappij die in rap tempo digitaliseert en globaliseert, ontstaan dagelijks nieuwe risico's. Dit verlangt dat organisaties flexibel moeten zijn en processen agile moeten worden ingericht. Maar tegelijkertijd biedt dit ook kansen. Kansen om nieuwe markten te betreden, sneller in te spelen op veranderende omstandigheden en bestaande en nieuwe risico's op een slimmere manier te beheersen.

Ook de maatschappelijke belangstelling voor good governance is onverminderd groeiend en levert interessante discussies op in relatie tot verantwoordelijkheden tussen commissaris en directie.

Het onderwerp risicomanagement leverde tijdens de interviews zoveel discussie op bij commissaris, directie en internal auditor dat een apart rapport voor dit onderwerp ons de beste keus leek. Bovendien hebben de recente ontwikkelingen rond de corona-crisis en de daarop volgende sociale en economische gevolgen alleen nog meer manifest gemaakt dat risicomanagement uitermate belangrijk is.

Het beeld is duidelijk. Commissarissen, directies en internal auditors vinden dat rvc's voldoende aandacht moeten besteden aan risicomanagement. Ook zijn zij van mening dat voor de meeste impactvolle calamiteiten, draaiboeken wenselijk zijn.
Wat opviel is dat de geïnterviewden veel vragen stelden over risicobeheersing en de indruk gaven dat zij zich gaandeweg realiseerden, dat binnen hun organisatie risicomanagement mogelijk niet voldoende is geactualiseerd en dat de relatie tussen geïdentificeerde risico's en (de effectiviteit van) geïmplementeerde beheersingsmaatregelen niet altijd transparant is. Bij nader inzien was er de nodige twijfel of voor calamiteiten, wel de juiste draaiboeken aanwezig zijn en in hoeverre de draaiboeken zijn geactualiseerd.

De hoofdconclusies van deze rapportage over risicomanagement zijn als volgt:

1. Duidelijke noodzaak voor verbeteren draaiboek/noodscenario's bij calamiteiten/ risicogebieden.
2. De belangrijkste risico's betreffen: strategie, informatiebeheer, digitalisering, grote eenmalige projecten, reputatie en betrouwbaarheid financiële rapportage, politiek, HR, markt, compliance en day-to-day business en regulator.
3. Voorkeur voor uitspraak van internal auditor boven die van externe accountant, behalve voor uitspraken over de betrouwbaarheid van de financiële rapportages en sommige financiële risico's.

We wensen u veel leesplezier en zijn graag beschikbaar om in geval van vragen naar aanleiding van dit rapport met u over risicomanagement in gesprek te gaan.

Björn Roskott
Partner risk management
Grant Thornton

Samenvatting

1. Duidelijke noodzaak voor verbeteren draaiboek noodscenario's bij calamiteiten/risicogebieden.
2. De belangrijkste risico's betreffen: strategie, informatiebeheer, digitalisering, grote eenmalige projecten, reputatie en betrouwbaarheid financiële rapportage, politiek, HR, markt, compliance en day-to-day business en regulator.
3. Voorkeur voor uitspraak van internal auditor boven die van externe accountant, behalve voor uitspraken over de betrouwbaarheid van de financiële rapportages en sommige financiële risico's.

Ad 1: duidelijke noodzaak voor verbeteren draaiboek/noodscenario's bij calamiteiten/risicogebieden

Voor alle benchmarks gezamenlijk is het **veranderpercentage** voor de wenselijkheid van het hebben van een draaiboek bij diverse calamiteiten/risicogebieden met 57 procent **zeer fors**. Bij de **bedrijfsbenchmarks** is dit met 67 procent hoger dan bij de **persoonsgebonden** profielen met 48 procent.

De **meest gedeelde veranderwensen** bij de 18 benchmarks betreffen de risicogebieden: verongelukken CEO en voorzitter rvc, publiek optreden van een klokkenluider en handelen in strijd met de principes van duurzaam ondernemen en negatieve publiciteit.

De **benchmarks** met de **hoogste veranderpercentages** zijn: het familiebedrijf, de onderwijssector, de zorgsector, de internal auditor en de commissaris bij een bedrijf zonder internal auditor.

Ad 2: belang risico's

Bijna de helft van de onderzochte risico's (12 van de 25) scoort bij minimaal 75 procent van de onderscheiden 18 benchmarks '**zeker van belang**' of hoger. Dit zijn, met tussen haakjes het procentueel aantal benchmarks dat daaraan voldoet:

- strategie, informatiebeheer, digitalisering, grote eenmalige projecten, reputatie en betrouwbaarheid financiële rapportage (elk 100);
- politiek (breed: lokaal tot en met internationaal) en HR (elk 94);
- markt en compliance (wet- en regelgeving) (elk 89); en
- day-to-day business en regulator (elk 83).

Het **belang** voor inflatie (0) en inkoop (6) bevindt zich aan de andere kant van het spectrum en is **afwezig** of **erg laag**.

Bij de **bedrijfsgebonden benchmarks** valt 18 procent in de categorie (**zeer**) **belangrijk** en bij de persoonsgebonden profielen 46 procent.

Ad 3: draagvlak voor uitspraak over onderzochte risico's

Internal auditor

Bij meer dan 75 procent van de benchmarks wordt variërend van **min of meer mee eens** tot beslist mee eens ermee ingestemd dat de internal auditor een uitspraak doet over de risico's bij:

- grote eenmalige projecten en informatiebeheer;
- handelen in strijd met gedragscode bedrijf, betrouwbaarheid financiële rapportage en compliance wet- en regelgeving;
- day-to-day business; en
- financieel risico (onder andere rente, valuta, debiteuren en liquiditeit).

Het **draagvlak** voor uitspraken van de internal auditor is **laag** tot **afwezig** voor: milieu en klimaat, inkoop, innovatie, markt, HR, politiek en inflatie.

De externe accountant

Bij meer dan 75 procent van de benchmarks wordt variërend van **min of meer mee eens** tot beslist mee eens ermee ingestemd dat de externe accountant een uitspraak doet over de risico's bij:

- betrouwbaarheid financiële rapportage en informatiebeheer;
- financieel risico (onder andere rente, valuta, debiteuren en liquiditeit);
- compliance wet- en regelgeving en grote eenmalige projecten; en
- financieel risico (onder andere disruptie financieel systeem).

Het **draagvlak** voor uitspraken van de externe accountant is **laag** tot **afwezig** voor: strategie, day-to-day business, politiek, samenwerking met externe (keten)partners en reputatie, outsourcing en markt. Innovatie, inflatie, HR, milieu en klimaat en inkoop scoren zelfs bij geen van de benchmarks een 3.5 of hoger.

Internal auditor en externe accountant ten opzichte van elkaar

In het algemeen bestaat er een **voorkeur** dat de **internal auditor** een **uitspraak** doet **over** de **risico's**. De internal auditor is hier zelf(s) zeer uitgesproken in. Alleen de **directie** heeft grosso modo een voorkeur voor de externe accountant. Wel blijkt bij de meeste benchmarks dat over de **betrouwbaarheid** van de **financiële rapportage** de **externe accountant** eerder in de lead zit dan de internal auditor. Deze laatste vindt dat zelf ook. De positie van de **internal auditor valt primair binnen de kaders/muren van de eigen organisatie**. Daarmee wordt een 'interne' oriëntatie gestimuleerd. In iets mindere mate lijkt dit op te gaan voor de externe accountant. **Niet onbelangrijke risico's** als marktrisico, reputatierisico, innovatierisico en HR-risico dreigen **buiten** de '**scope**' van beide spelers te vallen.

Discussievragen naar aanleiding van het onderzoek

1. Valt bekendheid met draaiboeken op risicogebieden niet onder de toezichtfunctie van de rvc?
2. Hoe zeker weten rvc, rvb, secretaris of internal auditor dat er een actueel draaiboek is?
3. Waarom is een draaiboek voor terrorisme minder wenselijk dan draaiboeken voor diverse andere risicogebieden?
4. Is klimaat-/milieurisico echt niet belangrijk?
5. Wordt aan integratierisico wel tijdig, voldoende en de juiste aandacht geschonken?
6. Nemen rvc en rvb signalen van internal auditor op de diverse risicogebieden wel serieus?
7. Doorgaans is er een voorkeur voor uitspraken over diverse risicogebieden van de internal auditor boven de externe accountant. Is er geen plaats voor externe accountant vanwege de (veronderstelde) kwaliteit en/of de prijs en/of onbekendheid met de dienstverlening?
8. Wie doet er uitspraken over bepaalde risicogebieden als externe accountant en internal auditor dat niet doen (bijvoorbeeld over markt-, HR- of over politiek risico)?
9. Waarom geen draaiboek voor het verongelukken van de voorzitter van de rvc?
10. Wordt wel eens nagedacht over Murphy's law in casu samenvallen van risico's?

Summary

1. Clear need for improved contingency/emergency plans in case of calamities/risk areas.
2. The most important risks relate to strategy, information management, digitalisation, large one-off projects, reputation and reliability of financial reporting, politics, HR, market, compliance, day-to-day business and the regulator.
3. Preference for the internal auditor's opinion over that of the external auditor, except with regard to opinions on the reliability of financial reporting and some financial risks.

Sub 1: clear need for improved contingency /emergency plans in case of calamities/risk areas

For all the benchmarks together, the **change percentage** for the desirability of having a contingency plan for various calamities/risk areas is **very substantial**, at 57 percent. Among the **company-specific benchmarks,** it is higher (67 percent) than among the **person-specific** profiles (48 percent).

The **desire for change most commonly shared** by the 18 benchmarks relates to the risk areas: accidental death of the CEO or Chairman of the Supervisory Board, public action by a whistle-blower, acts contrary to the principles of sustainable entrepreneurship and negative publicity. The **benchmarks** with the **highest change percentages** are family businesses, the education sector, the healthcare sector, internal auditors and supervisory directors at companies without an internal auditor.

Sub 2: importance of risks

Almost half of the risks included in the survey (12 out of 25) score **'definitely of importance'** or higher with at least 75 percent of the 18 different benchmarks. The risks in question are listed below, with the percentage of benchmarks awarding this score given in brackets:

- strategy, information management, digitalisation, large one-off projects, reputation and reliability of financial reporting, (each 100);
- politics (local to international) and HR (each 94);
- market and legal and regulatory compliance (each 89); and
- day-to-day business and regulator (each 83).

The **importance** awarded to the risk of inflation (0) and procurement (6) is at the other end of the spectrum and is either **absent** or **very low**.

Among the **company-specific benchmarks**, 18 percent fall into the category of (very) important and among the person-specific profiles, the relevant percentage is 46.

Sub 3: support base for opinions on the risks included in the survey

The internal auditor

More than 75 percent of the benchmarks agree – with the level of agreement varying from '**more or less agree**' to 'strongly agree' – that the internal auditor should express an opinion on the risks associated with the following:

- large one-off projects and information management;
- acts in violation of the company's code of conduct, reliability of financial reporting and legal and regulatory compliance;
- day-to-day business; and
- financial risks (e.g. interest, exchange rate, debtors and liquidity).

Support for the internal auditor expressing an opinion is **low** to **absent** for: environment and climate, procurement, innovation, market, HR, politics and inflation.

The external auditor

More than 75 percent of the benchmarks agree – with the level of agreement varying from '**more or less agree**' to 'strongly agree' – that the external auditor should express an opinion on the risks associated with the following:

- reliability of financial reporting and information management;
- financial risks (e.g. interest, exchange rate, debtors and liquidity)
- legal and regulatory compliance and large one-off projects; and
- financial risk (e.g. disruption of the financial system).

Support for the external auditor expressing an opinion is low to absent for: strategy, day-to-day business, politics, working with external (chain) partners and reputation, outsourcing and the market. Innovation, inflation, HR, environment and climate and procurement do not even score 3.5 or higher with any of the benchmarks.

Internal auditor and external auditor compared with each other

In general, there is a **preference** for the **internal auditor** to express an **opinion about the risks**. De internal auditor him/herself is very much in favour of this. Broadly speaking, only the **Management Board** has a preference for the external auditor. However, when it comes to the **reliability of financial reporting**, the **external auditor** is more likely to lead than the internal auditor, according to most benchmarks. The internal auditor him/herself also takes that view.

The **internal auditor primarily focuses on areas within the framework/walls of his/her own organisation. This encourages an 'internal' orientation**. To a slightly lesser extent, this also seems to apply to the external auditor. **A number of not-insignificant risks** such as market risk, reputational risk, innovation risk and HR risk are in danger of falling outside the scope of both auditors.

Questions for debate based on the results

1. Does the Supervisory Board's supervisory role not include familiarity with contingency plans for risk areas?
2. How sure are the Supervisory Board, the Board of Directors, the Secretary and the internal auditor that there is an up-to-date contingency plan?
3. Why is a terrorism contingency plan less desirable than contingency plans for various other risk areas?
4. Is climate/environmental risk really not important?
5. Is integration risk taken into account in a timely, sufficient and appropriate manner?
6. Do the Supervisory Board and the Board of Directors take signals from internal auditors in the various risk areas seriously?
7. In most cases, the internal auditor's opinion on various risk areas is preferred to that of the external auditor. Is there no room for an external auditor because of the (assumed) quality and/or the price and/or unfamiliarity with the service?
8. Who expresses an opinion on certain risk areas (e.g. market, HR or political risk) if the external and internal auditor do not?
9. Why is there no contingency plan in case of the accidental death of the Chairman of the Supervisory Board?
10. Does the organisation ever take Murphy's Law under consideration - in this case, the coincidence of risks?

1 Inleiding

1.1 Aanpak in dit onderzoek

Repeterende vragen en capita selecta

Dit onderzoek kent een **vergelijkbare aanpak** als de voorgaande jaarlijkse onderzoeken van 2008 tot en met 2018. Er wordt veelal gewerkt met een aantal repeterende vragen en wat capita selecta. Dit jaar is als speciaal onderwerp onder andere aandacht geschonken aan **risicomanagement**. Gezien de actualiteit van het onderwerp, de reacties van de geïnterviewden en de gevonden resultaten is besloten hiervan bij voorrang een deelrapport te laten verschijnen.

Respons gedaald, maar nog steeds hoog. 139 persoonlijke interviews

In totaal zijn er 269[3] vragenlijsten ingevuld die bruikbaar waren voor de kwantitatieve analyse. Hiervan waren er 207 commissarissen, 27 leden van de directie/rvb's, 12 secretarissen van rvc's en 23 internal auditors. Het aantal van 269 is statistisch qua aantallen vergelijkbaar met het aantal van 342 vorig jaar. In absolute termen en vergeleken met diverse andere onderzoeken is de respons nog steeds hoog, gezien ook de omvang van de vragenlijst.

Een deel van de vragenlijsten is ingevuld in combinatie met een **persoonlijk interview**. **Dit jaar zijn er 139 afgenomen**. Deze interviews zijn elke keer weer een bron van inspiratie en van zeer waardevolle informatie. Ze helpen ons om kritisch boven de 'getallen' uit te stijgen en de nodige nuanceringen aan te brengen bij de cijfermatige resultaten. De overige vragenlijsten zijn via een webbased vragenlijst ingevuld.

1.2 Verbijzondering resultaten naar basisprofiel en variaties daarop

Basisprofiel als referentiepunt

De structuur van de analyse is als volgt: Allereerst zijn de resultaten geanalyseerd voor een herkenbaar **basisprofiel** (toezichthouder bij beursgenoteerd bedrijf, gewoon lid van de rvc, zit in een two-tier board, geen lid rvb elders, ouder dan 55 jaar, man en geen lid van de auditcommissie). Daarna is de invloed van **variaties in het basisprofiel** op de resultaten geanalyseerd. Het voordeel van het werken met een basisprofiel is dat de resultaten beter kunnen worden geïnterpreteerd aan de hand van een **helder eenduidig profiel**. Ook de invloed van variaties in scores op het basisprofiel leveren extra inzicht op. Resultaten zijn hiermee onafhankelijk van de toevallige samenstelling van de groep commissarissen die de enquête heeft ingevuld. Hierdoor zijn de resultaten goed te vergelijken met de eerdere versies van dit onderzoek.

3 Om te voldoen aan de AVG-richtlijnen is een andere manier gekozen voor het benaderen van de respondenten van de andere, meewerkende organisaties. Dat is ons inziens de belangrijkste verklaring voor het teruglopen van de respons dit jaar.

Tabel 1 Onderscheiden (basisprofiel + variaties)/benchmarks en gehanteerde afkortingen

Bedrijfsprofielen/benchmarks		Persoonsgebonden profielen/benchmarks	
bapr	basisprofiel/beursgenoteerd bedrijf	**VZ**	voorzitter rvc/rvt
GB	groot niet-beursgenoteerd bedrijf	**'rvb'**	commissaris met rvb positie elders
MKB	midden- en kleinbedrijf	**Jong**	commissaris ≤ 55 jaar
Fam	familiebedrijf	**VR**	vrouwelijke commissaris
Corp	woningcorporatie	**AC**	commissaris lid auditcommissie
Zorg	zorginstelling		
OW	onderwijsinstelling	**Niet-commissarisprofielen/benchmarks**	
ONP	overige non-profit	**DIR**	lid rvb/directie
1tier	one-tier board	**Secr**	secretaris van de rvc
NOIA	geen internal auditor op payroll	**IA**	internal auditor

1.3 Regressieresultaten

De resultaten zijn verkregen met behulp van een **regressieanalyse**. Deze analyse destilleert uit 269 ingevulde enquêteformulieren, de resultaten voor het basisprofiel en de 'zuivere' effecten van variaties op het basisprofiel.

Voordelen regressieanalyse: inschatten basisprofiel en variaties onafhankelijk van exacte samenstelling groep respondenten

Het voordeel van deze regressieanalyse is driedelig:
De resultaten voor het basisprofiel en haar variaties kunnen worden verkregen zonder dat respondenten aan de exacte profielbeschrijving hoeven te voldoen.
De analyse is niet afhankelijk van de exacte **samenstelling van de groep respondenten**. Deze verschilt van jaar op jaar. Door elk jaar voor de verschillen in de samenstelling te controleren, kunnen de resultaten voor meerdere jaren goed met elkaar worden vergeleken.
De samenstelling van de groep respondenten is alleen van invloed op het significantieniveau van de resultaten voor het basisprofiel en de variaties. Als maar enkele rvc leden aan een beursgenoteerd bedrijf verbonden zijn, kunnen nauwelijks significante conclusies voor het basisprofiel worden getrokken. Daarom is met het benaderen van commissarissen en het afnemen van interviews aangestuurd op een evenwichtige samenstelling van de groep respondenten.

Invloed van variaties zijn bijna 'zuiver' te bepalen, ze zijn niet veel met elkaar gecorreleerd

Met regressieanalyses kunnen de **'zuivere' (of netto) invloeden** van de 17 variaties worden bepaald. Bijvoorbeeld, wanneer gemiddelde scores van beursgenoteerde bedrijven worden vergeleken met die van niet-beursgenoteerde, is het de vraag of de verschillen toe te schrijven zijn aan het niet-beursgenoteerd zijn of dat het ligt aan de gemiddeld kleinere omvang van de niet-beursgenoteerde bedrijven. De geschatte regressie coëfficiënten βV representeren nagenoeg de 'zuivere' effecten. Voorwaarde is wel dat de variaties niet teveel met elkaar gecorreleerd zijn, wat het geval is.

1.4 Woord van dank

De auteurs spreken hierbij hun dank uit naar alle commissarissen, leden rvb's/directies, secretarissen van rvc's en internal auditors voor hun medewerking (zie pagina 2).
De persoonlijke interviews van gemiddeld circa 2,5 uur leverden dit jaar weer een belangrijke toegevoegde waarde voor het verwerven van de nodige inzichten.
De respondenten uit het onderzoek zijn naast de eigen database via verschillende partners benaderd. Dit zijn: FBNed, Finem, de Governance University, de NCD, de NVTZ, de VTW, Topvrouwen.nl, VNO-NCW metropool Amsterdam en Stichting Blikverruimers en IIA Nederland. Léon de Man heeft de programmering en verzending van de webbased vragenlijst verzorgd.
Grant Thornton (www.grantthornton.nl) was ook dit jaar de **hoofdsponsor** van het commissarissen benchmarkonderzoek. **Cosponsor** was dit jaar IntegrationPeople.nl (www.integrationpeople.nl). De auteurs zijn en blijven Grant Thornton erkentelijk dat door deze samenwerking een bijdrage kan worden geleverd aan de ontwikkeling van het commissariaat in Nederland en ook dit jaar weer aan het métier van de internal auditors.

2 Risico's: belang, uitspraken internal auditor en externe accountant en calamiteiten

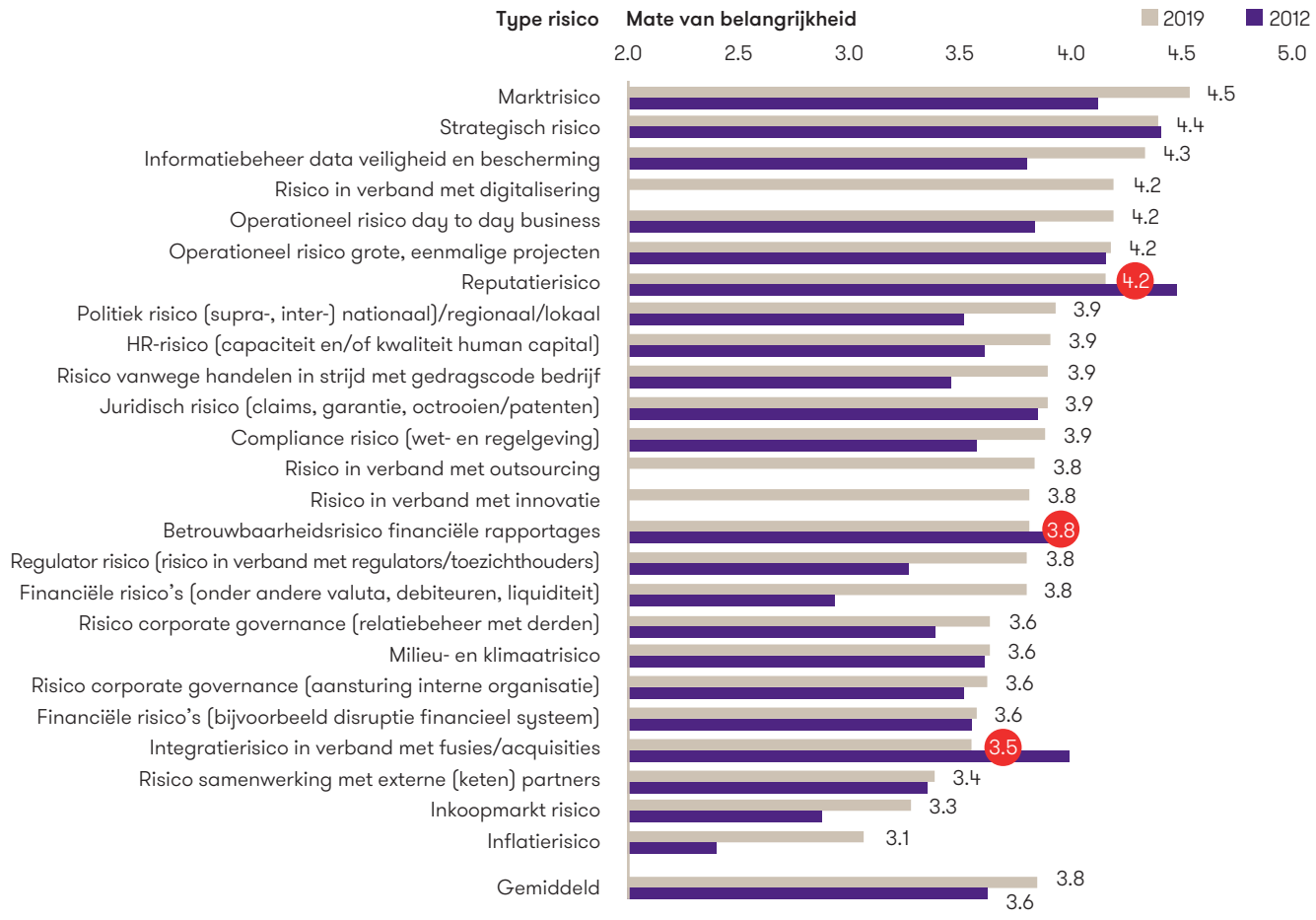
2.1 Inleiding

Onderzoeksvraag:
- **belang risico**
- **uitspraak internal auditor/externe accountant**
- **draaiboek bij calamiteiten**

In het 2012 benchmarkonderzoek is voor het eerst uitgebreid aandacht geschonken aan afzonderlijke risico's, rapportagefrequentie en kwantificering ervan. Besloten is dit jaar weer aandacht te schenken aan risico's. Daarbij zijn aan de orde gekomen: het **belang** van **afzonderlijke risico's**, de **wenselijkheid** van een **uitspraak** daarover van internal auditor en/of externe, controlerende accountant en de **aanwezigheid** van **draaiboeken/noodscenario's** bij een aantal **calamiteiten**. Bij de vraag over de draaiboeken is zowel naar de **huidige** als de **wenselijke situatie** gevraagd. Gebruik is gemaakt van een 5-puntsschaal met 1 = zeer onbelangrijk, 2 = onbelangrijk, 3 = deels onbelangrijk/deels belangrijk, 4 = belangrijk en 5 = zeer belangrijk. En een 5-puntsschaal met: 1 = volstrekt oneens, 2 = oneens, 3 = deels oneens/deels eens, 4 = mee eens en 5 = volstrekt mee eens.

2.2 Belang afzonderlijke risico's

Figuur 2.2 Belang afzonderlijke risico's basisprofiel



Legenda: de rood gearceerde getallen betreffen een fors lager belang voor de betrokken risico's in 2019. Verder hebben de getoonde scores betrekking op de resultaten van 2019.

Basisprofiel

Marktrisico zeer belangrijk; zes andere risico's belangrijk

Alleen **marktrisico** is **zeer belangrijk** (score ≥ 4.5).
In de categorie '**belangrijk**' (4.0 ≤ score belang < 4.5) vallen de risico's: **strategisch** risico, risico in verband met **informatiebeheer** data veiligheid en bescherming, risico in verband met **digitalisering**, **operationeel** risico **day-to-day** business, operationeel risico **grote eenmalige projecten** en **reputatierisico**.

60 procent van risico's 'zeker van belang'

In de categorie '**zeker van belang**' (3.5 ≤ score < 4.0) vallen 15 van de 25 expliciet genoemde risico's.
Het risico betreffende de samenwerking met externe (keten)partners en het inkoopmarktrisico valt in de categorie '**van belang**' (3.2 ≤ score < 3.5).

Inflatierisico laagste

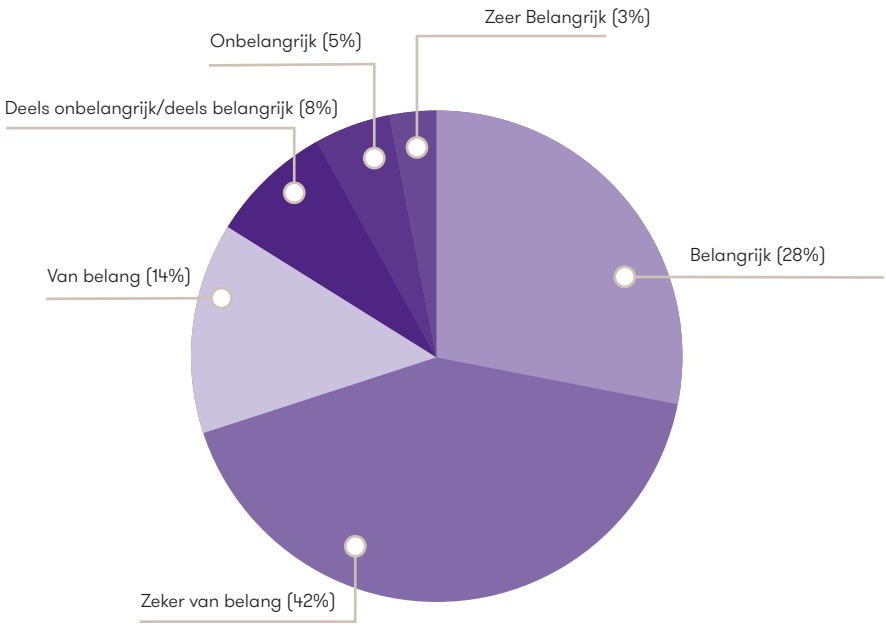
Het **inflatierisico** valt qua belang in de klasse '**deels onbelangrijk/deels belangrij**k'.

Basisprofiel: belang risico 2019 vergeleken met dat van 2012

Gemiddeld in 2019 hoger belang, maar lager voor risico: reputatie, integratie en betrouwbaarheid financiële rapportage

Gemiddeld scoren de opgenomen risico's in 2019 een 3.8 tegen 3.6 in 2012. Op een viertal risico's na is aan alle in beide onderzoeken opgenomen afzonderlijke risico's sprake van een (licht) hoger toegekend belang van het risico. Een **afnemend belang** valt waar te nemen bij **reputatierisico**, **betrouwbaarheidsrisico** financiële rapportages en bij **integratierisico** in verband met fusies/acquisities. Bij **strategisch risico** is dit verschil in absolute score verwaarloosbaar.
Een **fors hoger belang** en tevens leidend tot een andere kwalificatie van belang gaat op voor: **marktrisico** (+0.4 naar zeer belangrijk), **informatiebeheer** data veiligheid en bescherming (+0.5 naar belangrijk), **operationeel risico** day-to-day business (+0.4 naar zeker van belang), **regulator risico** (+0.5 naar zeker van belang), **financiële risico's** (onder andere valuta et cetera +0.9 naar zeker van belang) en het **inflatierisico** (+0.9). Dit laatste risico is nu deels onbelangrijk/deels belangrijk.

Clustering belang risico's alle benchmarks gezamenlijk



Overall is 70 procent van de risico's in de klassen 'zeker van belang' en '(zeer) belangrijk'

3 procent in 'zeer belangrijk' (score ≥ 4.5)
marktrisico (6 keer[4]), **strategisch risico** (3 keer), informatiebeheer data veiligheid en bescherming, operationeel risico (day-to-day business en eenmalige grote projecten), reputatierisico en politiek risico (elk 1 keer genoemd). In totaal is veertien keer een risico in deze klasse genoemd op een totaal van 450 opties (3 procent van totaal).
28 procent in 'belangrijk' (4.0 ≤ score < 4.5)
Informatiebeheer data veiligheid en bescherming (15 keer), risico in verband met **digitalisering** en **operationeel risico** grote eenmalige projecten (beide 12 keer), **reputatierisico** en **human resource** risico (capaciteit en kwaliteit human capital) (beide 11 keer), **strategisch** risico (10 keer) en **operationeel** risico day-to-day business (9 keer).

4 Tussen haakjes aantal benchmarks, waarop de kwalificatie van toepassing is.

De andere risico's in de categorie 'belangrijk' komen bij minder dan 50 procent van de benchmarks voor. In het totaal is 124 keer een risico geplaatst in deze klasse.
42 procent in 'zeker van belang' (3.5 ≤ score < 4.0)
Bij 50 procent of meer van de benchmarks vallen de volgende risico's in deze klasse: **betrouwbaarheidsrisico** financiële rapportage (16 keer), risico **corporate governance** (aansturing interne organisatie) (13 keer), **politiek** risico, **compliance** risico en **financiële** risico (onder andere rente, valuta liquiditeit) (elk 11 keer), **regulator** risico (10 keer), **juridisch** risico, risico in verband met **outsourcing** en **financiële risico** (disruptie in het financiële systeem) (elk 9 keer). In deze klasse gaat het om het 188 keer genoemd zijn van een risico.
14 procent in 'van belang' (3.2 ≤ score < 3.5)
Alleen **inkoopmarktrisico** (10 keer) komt in deze klasse bij meer dan 50 procent van de benchmarks voor. Risico's door **samenwerking** met **externe ketenpartners** (8 keer) en **financiële risico's** (disruptie van het financiële systeem) (7 keer) komen qua aantal benchmarks daarbij in de buurt. 65 keer is hier een risico in deze klasse genoemd.
8 procent in 'deels onbelangrijk/deels belangrijk' (2.8 ≤ score < 3.2)
In deze categorie is **inflatierisico** met acht keer het meest genoemd bij de afzonderlijke benchmarks. In totaal is 38 keer een risico in deze klasse geplaatst.
5 procent van de genoemde risico's kan voor de betrokken benchmarks als **(min of meer) onbelangrijk** (score < 2.8) worden beschouwd. Het betreft 21 keer genoemd zijn.

Gedeeld zijn van risico's in de klasse zeker van belang en hoger (tussen haakjes in procenten van totaal aantal benchmarks).

Zeer breed draagvlak voor relevantie bij twaalf risico's

Bij **meer dan 75 procent** van de benchmarks scoren een 3.5 of hoger de risico's bij:
- strategie, informatiebeheer, digitalisering, grote eenmalige projecten, reputatie en betrouwbaarheid financiële rapportage (elk 100);
- politiek en HR (elk 94);
- markt en compliance (wet- en regelgeving) (elk 89); en
- day-to-day business en regulator (elk 83).

Er is hier sprake van een zeer breed draagvlak variërend van 83 procent tot 100 procent.

Breed draagvlak voor relevantie bij negen risico's

Vanaf **50 procent tot 75 procent** van de benchmarks scoren een 3.5 of hoger de risico's bij:
- handelen in strijd met gedragscode bedrijf, juridisch, outsourcing, financieel risico (onder andere rente, valuta, debiteuren en liquiditeit), aansturing interne organisatie (elk 72);
- innovatie (67);
- relatiebeheer met overige partijen (61); en
- financieel risico (onder andere disruptie financieel systeem) en integratie fusies en acquisities (elk 50).

Het draagvlak voor het belang ligt nu lager, maar betreft nog 50 procent of meer van de benchmarks.

Lager maar nog wel substantieel tot geen draagvlak voor vier risico's

Minder dan 50 procent van de benchmarks scoort een 3.5 of hoger voor de risico's bij:
- milieu en klimaat (44);
- samenwerking met externe ketenpartners (39);
- inkoop (6); en
- inflatie (0).

Het draagvlak is nu aanzienzienlijk geringer, maar nog wel substantieel bij twee van de vier risicogebieden, namelijk milieu en klimaat en samenwerking met externe ketenpartners.

Andere benchmarks vergeleken met basisprofiel

Bij de bedrijfsbenchmarks 18 procent belangrijk en bij de persoonsgebonden 44 procent

In grote lijnen is het **belang** van de afzonderlijke **risico's bij** de **bedrijfsbenchmarks** doorgaans **lager** dan bij de persoonsgebonden benchmarks. Bij de bedrijfsbenchmarks valt zo'n 20 procent bij de **profitsector** in de klasse belangrijk met het **groot niet-beursgenoteerd** bedrijf als uitzondering met 8 procent. Bij de non-profitsector valt circa 15 procent in deze klasse met in dit geval de **woningcorporatie** als uitzondering naar boven met 20 procent.
Bij de **persoonsgebonden** profielen valt 46 procent in de klasse (zeer) belangrijk. Dit varieert van 46 procent bij de commissarissen tot 40 procent bij de niet-commissarissen.

Bij directie geen grote afwijkingen, wel wat andere classificaties

Enige opmerkelijke verschillen bij afzonderlijke benchmarks:
De afzonderlijke scores bij **directie wijken** in absolute zin **niet substantieel af** van die van het basisprofiel. Wel valt, anders dan bij het basisprofiel, een viertal risico's net in de hogere categorie 'belangrijk' bij de directie (handelen in strijd met de gedragscode, innovatie, outsourcing en HR). Net buiten deze categorie geldt dit voor day-to-day business bij de directie.
Milieu- en **klimaatrisico** is alleen bij de **vrouwelijke** commissaris belangrijk;
Het risico van **handelen** in strijd met de **gedragscode** van het **bedrijf** is bij de meeste **persoonsgebonden** profielen **belangrijk**. Bij de bedrijfsbenchmarks valt dit risico veelal in de categorie van hooguit 'van belang'.
Het **financiële risico** (onder andere rente, valuta, liquiditeit) is alleen bij de **woningcorporatie** en de **commissaris** elders lid **rvb** belangrijk.
Het **innovatierisico** is slechts belangrijk bij het familiebedrijf, voorzitter rvc en de vrouwelijke commissaris.
Het **betrouwbaarheidsrisico** van de **financiële rapportage** is alleen bij de 1tier en bij de commissaris lid van de auditcommissie belangrijk.
Het **integratierisico** is alleen bij **1tier** belangrijk.

Bij geen benchmark belangrijk

Verder scoren de volgende **risico's** bij **geen benchmark** een score in de categorie **belangrijk**: inflatierisico, inkoopmarktrisico, risico samenwerking met externe ketenpartners, integratierisico (fusies/acquisities/samenwerkingen), financiële risico's (onder andere disruptie financiële systeem) en beide risico's corporate governance.

Bespiegelingen/vragen/kanttekeningen

Is klimaat-/milieurisico echt niet belangrijk?

Wanneer wordt gekeken naar risico's zijn een paar zaken van belang, zoals wat is de kans dat een gebeurtenis zich voordoet? En als de gebeurtenis zich voordoet, wat is daarvan dan het gevolg? Enige losse opmerkingen willen wij met u delen naar aanleiding van de risicogebieden die expliciet zijn opgenomen in het onderzoek. Hoe hoog is de kans dat wij in Nederland of elders te maken krijgen met een tekort aan schoon drinkwater? Gezien het door de meeste benchmarks aangegeven belang van het klimaat-/milieurisico is de veronderstelde kans of niet groot en/of het effect verwaarloosbaar. Maar klopt dit wel? Als wij zien wat er elders in de wereld gebeurd is, zoals in Azië en Afrika bijvoorbeeld. Daar zijn sommige landen of belangrijke delen van landen verstoken van schoon drinkwater. Afgezien van klimatologische oorzaken, zijn ook ingrepen als bouwen van stuwdammen en andere wijze van irrigaties daaraan debet. Vertalen wij dat naar onze situatie. Door de waterwinningsmaatschappijen zijn diverse signalen afgegeven dat wij aan het interen zijn op ons grondwater, dat mede gebruikt wordt voor ons drinkwater. Niet uitgesloten is dat de rivieren, die door de andere landen stromen en ons onze grondstof drinkwater leveren, door landen die dichter bij de bronnen zitten, zo beïnvloed worden dat er minder water bij ons komt. Of niet op het gewenste moment. Zijn de huidige spelregels en de interpretatie daarvan om tot een verdeling te komen 'sustainable' genoeg? En als er echt keuzes moeten worden gemaakt, zijn wij dan wel de rationele, beschaafde mensheid in de verschillende landen? Wij weten het niet. Maar stel dat onze gedachte niet van enig realiteitsgehalte is ontbloot. En stel dat wij de signalen van de watermaatschappijen juist interpreteren. Hoe komt het dan dat zoveel andere personen, en dan denken wij primair aan de directies van de bedrijven en de commissarissen, behalve de vrouwelijke commissaris, milieu en klimaatrisico niet zo belangrijk vinden? Zien ze het niet? Willen ze het niet zien? Verwachten ze dat het probleem wel wordt getackeld? Of kijken ze teveel naar gisteren en negeren ze signalen en trends die wat over toekomstige ontwikkelingen zeggen?

Hoe belangrijk is het risico van sector- en/of bedrijfsblindheid?

De in het onderzoek opgenomen risicogebieden waren uiteraard niet limitatief. Zo hebben we bijvoorbeeld geen aandacht geschonken aan de bedrijfscultuur, de bestuurscultuur, bedrijfsblindheid en sectorblindheid. Over bedrijfs- en bestuurscultuur zijn in de loop van de tijd al veel wijsheden verkondigd. Daarom richten wij ons op de andere twee. U bent commissaris en heeft inmiddels drie commissariaten bij twee bedrijven uit de profitsector en één uit de non-profitsector. In alle drie de gevallen kwam u in een rvc die redelijk goed marcheerde, voor zover u dat kon bekijken. U heeft eerst de kat een beetje uit de boom gekeken en bent daarna full speed mee gaan draaien. Misschien heeft u voor uzelf wat aantekeningen gemaakt van wat u opviel. En misschien ook van wat u niet zinde bij de afzonderlijke commissariaten of wat u juist goed vond. Enige vragen: Hoe terdege heeft u uw due diligence gedaan alvorens toe te treden tot de betrokken rvc? Hoe belangrijk is het dat u een goede keuze maakt voor het commissariaat, waar u instapt? Wist u voordat u lid werd van de rvc welke cultuur er heerste in de raad en in het bedrijf? Zaten in de rvc voldoende mensen in met ervaring van buiten de sector? Of werd er heel sterk gehecht aan kennis van en ervaring met de sector? Hoort u geregeld 'bij dit bedrijf lopen de hazen zo'? Of 'dat is in deze sector niet gebruikelijk'? Neemt uzelf uw ervaringen en inzichten

verworven in het ene commissariaat wel in voldoende mate mee naar het andere commissariaat en vice versa? Misschien is het goed om met deze vragen in uw achterhoofd nog eens terug te kijken naar uw aantekeningen en naar de hiervoor en straks nog te verstrekken resultaten. Wij kunnen u verzekeren dat u niet de eerste en ook niet de laatste commissaris zult zijn, die het 'geleerde of het gebruik' in het ene commissariaat 'vergeet' mee te nemen naar het andere bedrijf. Is dat niet een vorm van bedrijfsblindheid?

Integratierisico is doorgaans best belangrijk, maar niet voor ons. Wij hebben de zaakjes op orde.

Met deze zin wordt een beetje het gevoel weergegeven die verschillende persoonlijke interviews dit jaar op dit risicogebied opriepen. Uit onderzoek blijken vele fusies/acquisities/samenwerkingen te mislukken. Bij de bedrijfsbenchmarks wordt het integratierisico in het algemeen met een kwalificatie 'van belang' als niet al te belangrijk gezien. Bij de persoonsgebonden profielen ligt dat belang doorgaans één klasse hoger in de categorie 'zeker van belang'. Er zijn weinig organisaties die niet te maken hebben met een of andere vorm van samenwerking en daarmee ook een vorm van integratie. De vraag is hoe het integratierisico wordt beoordeeld. Vermoedelijk wordt als maatstaf om succes of mislukken te meten in veel gevallen op een of andere manier in geld gedacht. Uiteraard kunnen ook andere doelstellingen als referentiekader dienen voor het bepalen van de mate van succes. En zeker geld in combinatie met wat boekhoudkundige vrijheden kan een vertekend beeld geven van de werkelijkheid. Imtech was destijds net als Aalberts Industries een bedrijf dat overname na overname deed en dat heel succesvol leek te doen. Bij Imtech bleek dat na een aantal jaren toch niet helemaal het geval. Bij Aalberts is een tijdje de rem gezet op de acquisities, omdat er volgens de huidige topman onder andere eerste aandacht besteed moest worden aan het 'verteren' van de acquisities. Wij vragen ons af hoe commissarissen en bestuurders bepalen of een acquisitie succesvol is of niet en hoe dat succes gemeten wordt.

Weten de jongere generaties wel wat inflatierisico is?

Van alle risico's wordt het inflatierisico doorgaans als het minst belangrijke gezien. Is de inflatie nu laag? In ons land nu wel. Blijft die laag? Geen idee. Krijgen wij een situatie, zoals in Japan? Misschien. Gaat de inflatie weer omhoog? Zeg nooit 'nooit'. En gaat dat stijgen eventueel geleidelijk of komt er opeens een versnelling? Wie het weet, mag het zeggen. Kijken we in bedrijven en organisaties nog wel naar inflatie? We weten het niet. Maar we zijn er niet op gerust. Er zijn historisch genoeg voorbeelden dat het historisch besef vaak een korte levensduur heeft. Waarom zou inflatie in ons land over, zeg vijf jaar, niet 8 procent kunnen zijn? Zijn er in het huidige tijdsbestek geen oorzaken te bedenken, die 'eergisteren' misschien irreëel waren, maar vandaag of nog beter gezegd morgen niet? Wordt er binnen uw bedrijf wel eens een scenario gemaakt om te zien in welke omstandigheden inflatie de kop weer kan opsteken en welke gevolgen dat dan heeft voor uw organisatie? In hoeverre heeft u in uw inkoop- en/of verkoopcontracten op voorhand al geprobeerd bepaalde risico's, samenhangend met inflatie in te dekken? Misschien eens overwegen, want iedereen vindt het risico niet belangrijk. Zou dat juist geen reden voor zorg moeten zijn?

2.3 Uitspraken over risico's door internal auditor en externe accountant

2.3.1 Uitspraken door internal auditor

Figuur 2.3.1 Wenselijkheid uitspraken door internal auditor: basisprofiel en internal auditor

Legenda: de rood gearceerde getallen betreffen een fors hogere mate van instemming bij de internal auditor en de oranje getallen een fors lagere mate van instemming bij de internal auditor voor uitspraken van de internal auditor. De getoonde cijfers in de figuur betreffen de scores van de internal auditor.

Eens met uitspraken van internal auditor bij zes risico's

Basisprofiel
In de categorie **'beslist mee eens'** (score ≥ 4.5) valt geen risico.
'duidelijk eens' met (4.0 ≤ score mate van instemming < 4.5) uitspraken door Internal auditor bij:
- operationeel risico, grote eenmalige projecten;
- informatiebeheer data veiligheid en bescherming;
- risico handelen in strijd met gedragscode van het bedrijf;
- betrouwbaarheid financiële rapportages;
- compliance risico (handelen in strijd met wet- en regelgeving); en
- operationeel risico day-to-day business.

In procentuele termen is dit 24 procent van het totaal aantal onderzochte risico's.

In de categorie **'min of meer mee eens'** (3.5 ≤ score < 4.0) vallen de uitspraken die in de figuur 2.3.1 zijn weergegeven met een score van 3.7 voor **integratierisico** in verband met fusies/acquisities tot en met 3.5 voor risico's in verband met **digitalisering**. In totaal vallen in deze klasse zeven risico's oftewel 28 procent van het totaal.

In de klasse 'neigt naar instemming' (3.2 ≤ score < 3.5) bevinden zich vijf risico's variërend van risico's door **samenwerking** met **externe** (keten)**partners** (3.48) tot en met **strategische risico's** (score 3.3). In procenten uitgedrukt is dit 20 procent van het totaal.

Het **inkoopmarkt** risico (score 3.15) en **milieu**- en **klimaatrisico** vallen in de **klasse 'deels oneens /deels eens'.** En in de klasse **'oneens'** zitten vijf risico's, namelijk het **HR-risico, risico in verband met 'innovatie', marktrisico, politiek risico en inflatierisico.** In het totaal zit 28 procent van de risico's in deze beide klassen.

Slechts bij drie van de zeven belangrijkste risico's een uitspraak van IA?

Relatie tussen belang van risico's en uitspraak van internal auditor bij basisprofiel
Het basisprofiel is er duidelijk mee eens dat de internal auditor over drie van de zeven (zeer) belangrijke risico's een uitspraak doet. Het betreft **grote eenmalige projecten**, **informatiebeheer** data veiligheid en bescherming en operationeel risico **day-to-day business**. **Over** het zeer belangrijke **marktrisico** en over **reputatie** en **strategie** worden (eigenlijk) **geen uitspraken** verwacht. Voor de risico's in verband met digitalisering vindt het basisprofiel een uitspraak min of meer wenselijk.
Daarmee lijkt een externe oriëntatie van de internal auditor niet te worden verwacht. De internal auditor 'moet' opereren binnen de 'context/muren' van de organisatie?

IA geen voorstander van uitspraak over de betrouwbaarheid financiële rapportage

Verschillen internal auditor met basisprofiel
De **internal auditors** zijn nog **stelliger** in hun mening **dan** het **basisprofiel** wat betreft de risico's, waarvan het basisprofiel vindt dat de internal auditor daarover een uitspraak doet. Het basisprofiel is het er duidelijk mee eens, de internal auditors zijn er zelfs **beslist mee eens** (score ≥ 4.5). Alleen een uitspraak over de betrouwbaarheid van de financiële rapportage laat een materieel verschil van mening zien. In tegenstelling tot het basisprofiel ziet de internal niet zo'n noodzaak (score 3.2) om daarover een uitspraak te doen.

IA ziet bij drie risico's geen rol en bij vier juist wel

Verder is de **internal auditor geen voorstander** van het doen van een **uitspraak** over: **juridische** risico's **en** de **financiële risico's**. Het basisprofiel ziet hier wel een rol voor de internal auditor.
Aan de andere kant voelt de **internal auditor** meer dan het basisprofiel voor het doen van een **uitspraak** over: risico corporate governance (**aansturing** van de **interne organisatie**), risico in verband met **outsourcing**, risico door **samenwerking** met externe **ketenpartners** en **reputatierisico**.

Bij zes van de tien belangrijkste risico's een uitspraak van IA

Relatie tussen belang van risico's en uitspraak van internal auditor bij internal auditor
De internal auditor zelf is het er (beslist) mee eens dat zij/hij bij zes van de elf door haar/hem aangegeven (zeer) belangrijke risico's een uitspraak doet. Dit betreft: informatiebeheer data veiligheid en bescherming, grote eenmalige projecten, handelen in strijd met de gedragscode, compliance (wet- en regelgeving), day-to-day business en outsourcing.
Voor de risico's in verband met reputatie, strategie en regulator vindt de internal auditor een uitspraak min of meer wenselijk. Dat geldt minder voor **digitalisering** en eigenlijk helemaal niet voor **marktrisico**.
Daarmee lijkt de internal auditor wat meer consistentie in haar/zijn antwoorden te hebben dan het basisprofiel. Wel is er tot op zekere hoogte een overeenstemming met de opvattingen, zoals waargenomen bij het basisprofiel. **Beide benchmarks** denken in **dezelfde richting** van risico's waarover een **uitspraak minder opportuun** wordt geacht.

4 procent beslist mee eens

Clustering uitspraken door internal auditor alle benchmarks gezamenlijk
In de categorie **'beslist mee eens'** (score ≥ 4.5) is slechts in **4 procent** van het totaal aantal mogelijke combinaties (= 450) een optie (= gewenste uitspraak over risico bij een benchmark) genoemd. Tot de genoemde uitspraken behoren: operationeel risico, grote **eenmalige projecten** (5 en 12 keer)[5], **informatiebeheer** data veiligheid en bescherming (4 en 13 keer), risico vanwege handelen in strijd met **gedragscode** van het bedrijf (3 en 7 keer), **betrouwbaarheid financiële rapportages** (1 en 11 keer), **compliance** risico (handelen in strijd met wet- en regelgeving) (2 en 11 keer) en operationeel risico **day-to-day business** (2 en 8 keer).

17 procent duidelijk mee eens

De klasse **'duidelijk mee eens'** (4.0 ≤ score mate van instemming < 4.5) telt **17 procent** van de genoemde opties. Het betreft vooral de hiervoor genoemde risico's. Daarnaast zijn een paar keer genoemd: **integratierisico** in verband met fusies/acquisities (3 en

5 Tussen haakjes staat het aantal benchmarks, waarop de kwalificatie van toepassing is voor 'beslist mee eens' (eerste getal) en de volgende categorie 'duidelijk mee eens' (tweede getal).

8 keer)[6], risico corporate governance (aansturing **interne organisatie** (2 en 8 keer), **financiële risico's** (onder andere rente, debiteuren en liquiditeit) (2 en 12 keer) en risico in verband met **digitalisering** (2 en 11 keer).

29 procent min of meer mee eens

In de categorie **'min of meer mee eens'** (3.5 ≤ score < 4.0) bevindt zich **29 procent** van de vermelde opties. Naast de hiervoor genoemde risico's betreft dit: handelen in strijd met de **gedragscode** van het bedrijf (7 keer)[7], **betrouwbaarheid financiële rapportages** (5 keer), **compliance** (wet- en regelgeving) (5 keer), **day-to-day** business (6 en 2 keer), **juridisch** risico (9 en 4 keer), **outsourcing** (12 en 2 keer), **regulator** (10 en 8 keer), **samenwerking** met (externe) **ketenpartners** (7 en 9 keer), **relatiebeheer** met overige partijen (5 en 6 keer), financieel risico (onder andere **disruptie** financieel systeem) (7 en 6 keer), **reputatierisico** (5 en 8 keer), **strategisch** risico (6 en 7 keer) en **milieu**- en **klimaat** (3 en 3 keer).

20 procent neigt naar instemming

In de klasse **'neigt naar instemming'** (3.2 ≤ score < 3.5) is **20 procent** van de genoemde opties. Naast de in de vorige klasse reeds genoemde risico's, zijn hier vaker dan één keer genoemd de risico's met betrekking tot: aansturing **interne organisatie** (7 keer), **digitalisering** (3 keer), **inkoopmarkt** (7 keer), **HR**-risico (4 keer), **innovatie** (3 keer) en **marktrisico** (6 keer).

Draagvlak voor uitspraken door internal auditor (tussen haakjes in procenten van totaal aantal benchmarks)

Zeer breed draagvlak voor uitspraken internal auditor bij zeven risico's

Bij meer dan **75 procent** van de **benchmarks** scoren de volgende risico's een **3.5 of hoger**:
- grote eenmalige projecten en informatiebeheer (elk 100);
- handelen in strijd met gedragscode bedrijf, betrouwbaarheid financiële rapportage en compliance wet- en regelgeving (elk 94);
- day-to-day business (89); en
- financieel risico (onder andere rente, valuta, debiteuren en liquiditeit) (78).

Er is hier sprake van een zeer breed draagvlak variërend van 100 procent tot 78 procent.

Breed draagvlak voor uitspraken bij zes risico's

Bij **50 tot 75 procent** van de **benchmarks** scoren de volgende risico's een **3.5 of hoger**:
- outsourcing en digitalisering (elk 72);
- integratie fusies en acquisities (61);
- aansturing interne organisaties, juridisch risico en regulator (elk 56).

Het draagvlak voor uitspraken van de internal auditor ligt nu lager, maar betreft nog meer dan 50 procent van de benchmarks.

Lager maar nog wel substantieel draagvlak voor vijf risico's

Bij **25 tot 50 procent** van de **benchmarks** scoren de volgende risico's een **3.5 of hoger:**
- samenwerking met externe ketenpartners (44);
- financieel risico (onder andere disruptie financieel systeem) (39);
- strategisch risico (33); en
- relatiebeheer met overige partijen en reputatierisico (elk 28);

Het draagvlak is nu aanzienzienlijk geringer maar nog wel substantieel.

Beperkt tot geen draagvlak voor uitspraken internal auditor bij zeven risico's

Minder dan 25 procent van de benchmarks scoren een **3.5 of hoger** bij de volgende risico's:
- milieu- en klimaat (17);
- inkoopmarkt (11);
- innovatie en marktrisico (elk 6); en
- HR, politiek en inflatie (elk 0).

6 Tussen haakjes staat nu het aantal benchmarks, waarop de kwalificatie van toepassing is voor 'duidelijk mee eens' (eerste getal) en de volgende categorie 'min of meer mee eens' (tweede getal).

7 Tussen haakjes staat nu het aantal benchmarks, waarop de kwalificatie van toepassing is voor de besproken categorie (enig getal of eerste getal) en de volgende categorie (tweede getal).

Bespiegelingen/vragen/kanttekeningen

Moet ook de internal auditor een uitspraak doen over de betrouwbaarheid van de financiële rapportage?
Onder andere het basisprofiel is duidelijk van mening dat ook de internal auditor een uitspraak moet doen over de betrouwbaarheid van de financiële rapportage (=BFinRap). De internal auditor vindt dat minder vanzelfsprekend en vindt dat deze taak als één van de weinige primair op het bordje moet liggen van de externe accountant. Waarom hecht een commissaris zo aan een uitspraak van en een internal auditor en een externe accountant over de BFinRap? Past dat in het risicomijdend gedrag van Nederlanders en sluit het aan bij onze verzekeringsbereidheid en zo ook bij commissarissen? Komt het omdat de commissarissen onvoldoende vertrouwen hebben in het onderliggende proces en de mensen die erbij betrokken zijn? Of heeft het te maken met hun eventuele, persoonlijke reputatieschade en/of aansprakelijkheid, als er wel iets niet lijkt te kloppen? Of hebben ze geen fiducie in de externe accountant? Of denken ze dezelfde kwaliteit te kunnen bereiken met de inzet van de internal auditor, maar dan tegen een lagere prijs bij de externe accountant? Overigens wordt het risico van BFinRap nagenoeg bij geen benchmark als (zeer) belangrijk gezien. En toch de dubbele dekking! Of hangt dit wellicht samen met de historische en wettelijke oriëntatie dat een commissaris décharge moet worden verleend voor het gehouden toezicht? Aan de andere kant: wat is erop tegen dat de internal auditor hierover een uitspraak doet? Als de rvc en misschien ook de rvb daardoor rustiger kunnen slapen, is dat toch wel wat waard?

Nemen rvc en rvb signalen van internal auditor wel serieus?
Wij geven de rvc en rvb in overweging, om de door de internal auditor geuite wensen, ook uitspraken te doen over risicogebieden als bijvoorbeeld aansturing van de interne organisatie, samenwerking met externe ketenpartners en outsourcing serieus te nemen en eens onbevooroordeeld te bespreken. Op grond van onze ervaringen met diverse evaluaties van rvc's en onze persoonlijke interviews, kunnen wij ons niet aan de indruk onttrekken, dat er op dit gebied verbetermogelijkheden liggen voor het goed uitoefenen van de taken van de rvc.

Kijkt internal auditor wel voldoende van buiten naar binnen?
Op grond van eerder onderzoek en ook op grond van het voorliggende onderzoek kunnen wij ons niet aan de indruk onttrekken dat de wereld van de internal auditor, zowel door de internal auditor zelf als door de rvb en rvc te eng geplaatst wordt, binnen de muren/kaders van het bedrijf. Over marktrisico en politiek risico worden bijvoorbeeld nauwelijks uitspraken verwacht van de internal auditor. Ook de instemming met uitspraken over reputatie en strategie behoort niet tot de 'top-categorie'. Wij bepleiten wat dat betreft een bredere oriëntatie.

2.3.2 Uitspraken door externe accountant

Figuur 2. 3.2 Wenselijkheid uitspraken externe accountant: basisprofiel en internal auditor

Legenda: het rood gearceerde getal betreft een fors hogere mate van instemming bij de internal auditor en de oranje getallen een fors lagere mate van instemming bij de internal auditor voor uitspraken van de externe accountant. De getoonde getallen betreffen die van de internal auditor.

Duidelijk eens met uitspraken van externe accountant bij drie risico's

Bij 36 procent van de risico's ≥ min of meer eens met uitspraak van externe accountant

Basisprofiel

In de categorie '**beslist mee eens**' (score ≥ 4.5) valt betrouwbaarheid financiële rapportage.

'**duidelijk eens**' **met** (4.0 ≤ score mate van instemming < 4.5) uitspraken door externe accountant bij:

- informatiebeheer data veiligheid en bescherming; en
- compliance risico (handelen in strijd met wet- en regelgeving).

In totaal vallen in deze beide klassen **drie risico's** oftewel **12 procent** van het totaal.

In de categorie '**min of meer mee eens**' (3.5 ≤ score < 4.0) vallen de uitspraken voor **financiële** risico's (onder andere rente, debiteuren, liquiditeit), grote eenmalige projecten, handelen in strijd met gedragscode, juridisch risico, financiële risico's (onder andere disruptie financiële systeem) en aansturing interne organisatie. Deze zes risico's zijn goed voor **24 procent** van het totaal.

In de klasse '**neigt naar instemming**' (3.2 ≤ score < 3.5) bevinden zich eveneens zes risico's en wel: regulator risico, integratierisico, relatiebeheer met overige partijen, digitalisering, day-to-day business en outsourcing. In procenten uitgedrukt is dit ook 24 procent van het totaal.

Strategie, samenwerking met externe (keten)partners en reputatie vallen in de klasse '**deels oneens /deels eens**'. En in de klasse '**oneens**' zitten zeven risico's, namelijk inkoopmarkt, markt, milieu- en klimaat, HR, inflatie, politiek en innovatie. In het totaal zit **40 procent** van de risico's in deze beide laatste klassen.

Relatie tussen belang van risico's en uitspraak van externe accountant bij basisprofiel

Het basisprofiel vindt dat de externe accountant **beslist** een **uitspraak** moet doen

over de **betrouwbaarheid** van de **financiële rapportages**. Het risico bij dit onderwerp is 'slechts' zeker van belang. Over het zeer belangrijke marktrisico hoeft de externe accountant geen uitspraak te doen. Hetzelfde geldt in iets mindere mate voor de 'belangrijke' risico's ten aanzien van strategie en reputatie. Van de drie resterende 'belangrijke' risico's wordt zeker een uitspraak verwacht over informatiebeheer data veiligheid en bescherming en over compliance (wet- en regelgeving). Over grote eenmalige projecten is de gedachte dat de accountant daarover min of meer ook een uitspraak doet.

Internal auditor ziet maar beperkte rol voor externe accountant

Internal auditor vergeleken met basisprofiel over uitspraken door externe accountant

Bij **60 procent** van de risico's is er materieel **geen verschil** van opvattingen tussen het basisprofiel en de internal auditor over het doen van uitspraken door de externe accountant over de onderzochte risico's.

Ook de internal auditor vindt dat de externe accountant **beslist** een **uitspraak** moet doen over de **betrouwbaarheid** van de **financiële rapportages**. In de categorie 'duidelijk mee eens' heeft de internal auditor geen uitspraak van de externe accountant geplaatst en in de categorie '**min of meer mee eens**' slechts **drie**, namelijk over: **informatiebeheer** data veiligheid en bescherming, corporate governance (**aansturing interne organisatie**) en **financiële risico's** (onder andere rente, valuta, liquiditeit). In het totaal komt de internal auditor daarmee op 16 procent van de uitspraken van de externe accountant, die in ieder geval in de klasse 'min of meer instemming' valt tegen 36 procent bij het basisprofiel. De **conclusie** is dat de internal auditor slechts een beperkte rol ziet weggelegd voor de externe accountant.

Externe accountant ook niet in beeld bij (zeer) belangrijke risico's

Relatie tussen belang van risico's bij internal auditor en uitspraak door de externe accountant

Voor slechts één van de (zeer) belangrijke risico's bij de internal auditor is deze het 'min of meer eens' met een uitspraak van de externe accountant en wel bij '**informatiebeheer** data veiligheid en bescherming'. Bij vijf van deze risico's neigt de internal auditor naar instemming. En bij vier is zij/hij het er deels mee oneens/deels eens. Voor het belangrijke marktrisico is voor beiden geen rol weggelegd.

Beslist mee eens voor betrouwbaarheid financiële rapportage

Clustering uitspraken door externe accountant alle benchmarks gezamenlijk

In de categorie '**beslist mee eens**' (score ≥ 4.5) is slechts in **4 procent** van het totaal aantal mogelijke combinaties (= 450) een optie (= gewenste uitspraak over risico bij een benchmark) genoemd. Vijftien van de zeventien uitspraken betreffen de betrouwbaarheid van de financiële rapportages. Compliance (wet- en regelgeving) en grote eenmalige projecten zijn elk één keer genoemd. Het beeld is daarmee aanzienlijk overzichtelijker dan bij de internal auditor.

12 procent duidelijk mee eens

De klasse '**duidelijk mee eens**' (4.0 ≤ score mate van instemming < 4.5) telt 12 procent van de genoemde opties. Het betreft **vooral**: **informatiebeheer** data veiligheid en bescherming (13 en 5 keer)[8] en **compliance** (12 en 3 keer).

Minder vaak in deze klasse zijn genoemd: financiële risico's (onder andere rente, debiteuren en liquiditeit) (3 en 14 keer), grote eenmalige projecten (5 en 10 keer), juridisch (4 en 9 keer) en financiële risico's (onder andere disruptie financieel systeem) (4 en 11 keer).

24 procent min of meer mee eens

In de categorie '**min of meer mee eens**' (3.5 ≤ score < 4.0) bevindt zich 24 procent van de vermelde opties. Naast de hiervoor genoemde risico's betreft dit: handelen in strijd met de gedragscode van het bedrijf (6 en 6 keer)[9], aansturing interne organisatie (10 en 4 keer), regulator (6 en 9 keer), integratie (fusie, acquisitie, samenwerking) (5 en 3 keer), relatiebeheer met overige partijen (7 en 4 keer) en digitalisering (11 en 4 keer).

16 procent neigt naar instemming

In de klasse '**neigt naar instemming**' (3.2 ≤ score < 3.5) is 16 procent van de genoemde opties. Naast de in de vorige klasse reeds genoemde risico's zijn hier vaker dan drie keer genoemd de risico's met betrekking tot: **day-to-day business** (11 keer), **outsourcing** (7 keer), **strategie** en **reputatie** (elk 4 keer).

8 Tussen haakjes staat nu het aantal benchmarks, waarop de kwalificatie van toepassing is voor 'duidelijk mee eens' (eerste getal) en de volgende categorie 'min of meer mee eens' (tweede getal).

9 Tussen haakjes staat nu het aantal benchmarks, waarop de kwalificatie van toepassing is voor 'min of meer mee eens' (enig getal of eerste getal) en de volgende categorie 'neigt naar instemming' (tweede getal).

Zeer breed draagvlak voor uitspraken externe accountant bij zes risico's	**Draagvlak** voor uitspraken door externe accountant (tussen haakjes in procenten van totaal aantal benchmarks). Bij meer dan 75 procent van de benchmarks scoren de volgende risico's een 3.5 of hoger: • betrouwbaarheid financiële rapportage en informatiebeheer (elk 100); • financieel risico (onder andere rente, valuta, debiteuren en liquiditeit) (94); • compliance wet- en regelgeving en grote eenmalige projecten (elk 89); en • financiële risico's (onder andere disruptie financieel systeem (83). Er is hier sprake van een zeer breed draagvlak variërend van 100 tot 83 procent.
Breed draagvlak voor uitspraken bij vier risico's	Bij 50 tot 75 procent van de benchmarks scoren de volgende risico's een 3.5 of hoger: • juridisch risico en aansturing interne organisaties (elk 72); • digitalisering (61); en • handelen in strijd met de gedragscode (50). Het draagvlak voor uitspraken van de internal auditor ligt nu lager, maar betreft nog 50 procent tot 75 procent van de benchmarks.
Lager maar nog wel substantieel draagvlak voor drie risico's	Bij 25 tot 50 procent van de benchmarks scoren de volgende risico's een 3.5 of hoger: • regulator; • integratie (fusie, acquisitie, samenwerking); en • relatiebeheer met overige partijen. Het draagvlak is met 39 procent bij elk van de risicogebieden aanzienzienlijk geringer maar nog wel substantieel.
Beperkt tot geen draagvlak voor uitspraken externe accountant bij zeven risico's	Bij de overige, hier niet genoemde, risico's scoort minder dan 25 procent van de benchmarks een 3.5 of hoger. Het betreft strategie (22), grote eenmalige projecten (17), samenwerking met externe (keten)partners en reputatie (elk 11), outsourcing en markt (elk 6). Er zijn zelfs vijf risico's die bij geen van de benchmarks een 3.5 of hoger scoren. Dit betreft: innovatie, inflatie, HR, milieu en klimaat en inkoop.

Bespiegelingen/vragen/kanttekeningen

Geen plaats voor externe accountant vanwege (veronderstelde) kwaliteit en/of vanwege de kosten en/of onbekendheid?

De laatste jaren blijken diverse accountants-/adviesbureaus vooral in hun adviestak de nodige groei in omzet en resultaat te laten zien. Blijkbaar is er voor die diensten een goede markt. Ook investeren de bedoelde organisaties veelal substantieel in hun ontwikkeling. In de assurance tak speelt vermoedelijk de druk van de AFM een belangrijke rol bij deze investeringen. Bij de adviestak speelt ongetwijfeld de wens tot een verbreding van het businessmodel en de wens om onderscheidend vermogen op te bouwen. In accountantskringen wordt gesteld dat de eigen adviespraktijk belangrijk is voor de dienstverlening op het gebied van assurance. Het lijkt ons aannemelijk dat ook de organisaties van de respondenten van het onderzoek van beide diensten van accountants -/adviesorganisaties gebruik hebben gemaakt en maken. De vraag is dan of de kosten van die diensten ook op het netvlies van de commissaris en de internal auditor zijn gekomen. En misschien überhaupt of bepaalde diensten worden geleverd. Bij de directie is dat waarschijnlijk wel het geval, want die heeft relatief een voorkeur voor uitspraken van de externe accountant over de diverse risicogebieden boven die van de internal auditor. Vermoedelijk is de directie voor de adviesdiensten ook de primaire opdrachtgever. Voor de assurance-tak zou dat de auditcommissie moeten zijn. Naar we vernemen op basis van de interviews, is de praktijk op dit gebied wel wat fluïde. Niet elke auditcommissie en, bij afwezigheid van deze commissie, de rvc heeft de kwaliteiten in huis om een volwaardig gesprekspartner te zijn van de externe accountant. Een terugvallen op de rvb en dan veelal de CFO lijkt dan voor de hand te liggen. Een aantal vragen komt bij ons op. Is de rvc/auditcommissie op de hoogte van de diensten die de externe accountant kan bieden als ondersteuning voor het duiden van risico's? Kan de accountant inhoudelijk de risico's ook beoordelen, dat wil zeggen, begrijpt hij/zij waarover het gaat? Zijn de rvc en rvb bereid de prijs (= kosten) te betalen van de dienstverlening? In hoeverre kan de externe accountant de claim hard maken dat deze, doordat zij/hij bij verschillende relaties en uiteenlopende typen bedrijven komt, een meerwaarde biedt boven bijvoorbeeld de internal auditor? En geldt dat ook voor een externe accountant die alleen maar werkt voor een bepaalde sector als onderwijs, woningcorporatie of zorg?

2.3.3 Vergelijking uitspraken door internal auditor en externe accountant.

Basisprofiel

Tabel 2.3.3.1 Belang risico's en wenselijkheid uitspraken internal auditor en externe accountant bij basisprofiel

Risico	bapr	≥ 4.5	4 – 4.5		3.5 - 4		3.2 – 3.5		2.8 – 3.2		< 2.8	
	Belang		IA	EA	IA	EA	IA	EA	IA	EA	IA	EA
Markt	4.5										IA	EA
Strategie	4.4						IA			EA		
Informatiebeheer	4.3		IA	EA								
Digitalisering	4.2				IA			EA				
Day-to-day business	4.2		IA					EA				
Grote eenmalige projecten	4.2		IA					EA				
Reputatie	4.2						IA			EA		
Politiek risico	3.9										IA	EA
HR	3.9										IA	EA
Handelen in strijd met gedragscode	3.9		IA			EA						
Juridisch	3.9				IA	EA						
Compliance	3.9		IA	EA								
Outsourcing	3.8				IA			EA				
Innovatie	3.8										IA	EA
Betrouwbaarheid financiële rapportage	3.8	EA	IA									
Regulator	3.8				IA			EA				
Financiële risico's (onder andere rente, liquiditeit)	3.8				IA	EA						
Relatiebeheer met derden	3.6						IA	EA				
Milieu- en klimaat	3.6								IA			EA
Aansturing interne organisatie	3.6				IA	EA						
Financiële risico's (bijvoorbeeld disruptie financieel systeem)	3.6					EA	IA					
Integratie	3.5				IA			EA				
Samenwerking met externe partners	3.4						IA			EA		
Inkoopmarkt	3.3								IA			EA
Inflatie	3.1										IA	EA

Legenda

- In de eerste kolom zijn de afzonderlijke risico's genoemd in wat compactere vorm dan in de eerdere paragrafen van dit hoofdstuk.
- In de tweede kolom staat het belang van het risico, zoals aangegeven door het basisprofiel (= bapr), in afnemende mate van belang. De (zeer) belangrijke risico's hebben een kleur gekregen.
- In de volgende kolommen staan de gehanteerde klassen weergegeven voor de mate van instemming met een uitspraak door respectievelijk de internal auditor (= IA) en de externe accountant (= EA).

Doorgaans spreekt het **basisprofiel** met **meer stelligheid** uit dat de **internal auditor** bij een bepaald risico een **uitspraak** moet doen dan dat dit op het bordje ligt van de externe accountant.

Voorkeur voor internal auditor bij twaalf risico's

De internal auditor heeft bij **tien risico's** steeds **één hogere klasse** qua instemming en bij **twee zelfs twee**. Deze laatste twee gaan over de beide **operationele risico's**.
Bij **elf risico's** komen internal auditor en externe accountant in **dezelfde klasse** qua instemming. Hiervan hebben er vijf betrekking op de klasse dat een uitspraak niet nodig is door beide spelers.

Voorkeur externe accountant bij twee risico's

Bij **twee risico's** heeft de **externe accountant** de **voorkeur**, namelijk bij de betrouwbaarheid van de financiële rapportage en bij de financiële risico's (onder andere disruptie van het financieel systeem).

Internal auditor

Tabel 2.3.3.2 Belang risico's en wenselijkheid uitspraken internal auditor en externe accountant bij internal auditor

Risico	bapr	≥ 4.5	4 – 4.5		3.5 - 4		3.2 – 3.5		2.8 – 3.2		< 2.8	
	Belang		IA	EA	IA	EA	IA	EA	IA	EA	IA	EA
Informatiebeheer	4.8	IA				EA						
Reputatie	4.6				IA			EA				
Digitalisering	4.4						IA			EA		
Handelen in strijd met gedragscode	4.3	IA						EA				
Grote eenmalige projecten	4.3	IA						EA				
Strategie	4.3				IA					EA		
Markt	4.2										IA	EA
Outsourcing	4.1		IA							EA		
Compliance	4.1	IA						EA				
Day-to-day business	4.1	IA								EA		
Regulator	4.0				IA			EA				
HR	3.9								IA			EA
Financiële risico's (onder andere rente, liquiditeit)	3.9					EA					IA	
Juridisch	3.8								IA	EA		
Politiek risico	3.8										IA	EA
Betrouwbaarheid financiële rapportage	3.7	EA					IA					
Innovatie	3.7								IA			EA
Aansturing int. organisatie	3.6		IA			EA						
Relatiebeheer met derden	3.6						IA	EA				
Financiële risico's (bijvoorbeeld disruptie financieel systeem)	3.6							EA			IA	
Samenwerking met externe partners	3.5				IA							EA
Milieu- en klimaat	3.4						IA					EA
Inkoopmarkt	3.2		IA							EA		
Integratie	3.1				IA					EA		
Inflatie	2.7										IA	EA

Legenda

- In de eerste kolom zijn de afzonderlijke risico's genoemd in wat compactere vorm dan in de eerdere paragrafen van dit hoofdstuk.
- In de tweede kolom staat het belang van het risico, zoals aangegeven door de internal auditor (= IA), in afnemende mate van belang. De (zeer) belangrijke risico's hebben een kleur gekregen.
- In de volgende kolommen staan de gehanteerde klassen weergegeven voor de mate van instemming met een uitspraak door respectievelijk de internal auditor en de externe accountant (= EA).

Internal auditor ziet nauwelijks ruimte voor externe accountant

De internal auditor is zeer uitgesproken. Bij maar liefst 11 van de 25 risico's is het verschil tussen de mate van instemming met een uitspraak door de internal auditor en met die van de externe accountant twee klassen of meer. Bij zes risico's is het verschil één klasse.
Bij dertien risicogebieden met een instemming van 3.5 of meer ziet de internal auditor voor zichzelf een plaats tegen slechts vier voor de externe accountant.
Bij **drie risico's** heeft de **externe accountant** de **voorkeur**, namelijk bij de betrouwbaarheid van de financiële rapportage en bij de beide financiële risico's.
We vragen ons af of er sprake is van een 'jalousie de métier'?
Bij **vijf risico's** komen internal auditor en externe accountant in **dezelfde klasse** qua instemming. Hiervan hebben er drie betrekking op de klasse dat een uitspraak niet nodig is door beide spelers.
De internal auditor heeft bij tien risico's steeds één hogere klasse qua instemming en bij twee zelfs twee. Deze laatste twee gaan over de beide operationele risico's.

Commissaris lid auditcommissie

Tabel 2.3.3.3 Belang risico's en wenselijkheid uitspraken internal auditor en externe accountant bij commissaris lid audit commissie

Risico	AC	≥ 4.5	4 – 4.5		3.5 - 4		3.2 – 3.5		2.8 – 3.2		< 2.8	
	Belang		IA	EA	IA	EA	IA	EA	IA	EA	IA	EA
Markt	4.7								IA	EA		
Strategie	4.6				IA			EA				
Informatiebeheer	4.4	IA		EA								
Reputatie	4.4				IA			EA				
Grote eenmalige projecten	4.4	IA		EA								
Day-to-day business	4.3	IA				EA						
Compliance	4.2	IA		EA								
Digitalisering	4.2				IA	EA						
Handelen in strijd met gedragscode	4.1	IA				EA						
Politiek risico	4.1										IA	EA
HR	4.1						IA			EA		
Betrouwbaarheid financiële rapportage	4.1	EA	IA									
Regulator	4.0				IA	EA						
Juridisch	3.9				IA	EA						
Financiële risico's (onder andere rente, liquiditeit)	3.9				IA	EA						
Innovatie	3.9								IA			EA
Integratie	3.8		IA			EA						
Relatiebeheer met derden	3.8				IA	EA						
Outsourcing	3.8				IA			EA				
Aansturing interne organisatie	3.8		IA	EA								
Financiële risico's (bijvoorbeeld disruptie financieel systeem)	3.8					EA	IA					
Milieu- en klimaat	3.8						IA			EA		
Samenwerking met externe partners	3.8				IA					EA		
Inkoopmarkt	3.6								IA			EA
Inflatie	2.9										IA	EA

Legenda

- In de eerste kolom zijn de afzonderlijke risico's genoemd in wat compactere vorm dan in de eerdere paragrafen van dit hoofdstuk.
- In de tweede kolom staat het belang van het risico, zoals aangegeven door de commissaris lid Auditcommissie (= AC), in afnemende mate van belang. De (zeer) belangrijke risico's hebben een kleur gekregen.
- In de volgende kolommen staan de gehanteerde klassen weergegeven voor de mate van instemming met een uitspraak door respectievelijk de internal auditor (= IA) en de externe accountant (= EA).

Commissaris lid auditcommissie duidelijke voorkeur voor internal auditor

De commissaris lid auditcommissie neemt qua teneur eenzelfde positie in als de commissaris van het basisprofiel, namelijk een voorkeur om vooral terug te vallen op de internal auditor.

De **internal auditor** heeft bij **veertien** risico's steeds de voorkeur boven de externe accountant. Bij drie risico's is er sprake van twee **hogere klassen** qua **instemming**. Dit betreft: operationeel risico day-to-day business en handelen in strijd met gedragscode bedrijf (beslist eens met uitspraak door IA) en samenwerking met externe ketenpartners (min of meer mee eens). Bij elf risico's is de mate van instemming één klasse hoger. Het betreft nu de risico's bij: informatiebeheer, grote eenmalige projecten en compliance (beslist eens met uitspraak door IA), integratie (duidelijk mee eens), strategie, reputatie, outsourcing en externe ketenpartners (min of meer eens met uitspraak van IA). In de twee laatste klassen vallen: HR, milieu en klimaat, innovatie en inkoop.

Bij **negen risico's** komen de internal auditor en externe accountant in **dezelfde klasse** qua instemming. Hiervan hebben er twee betrekking op de klasse dat een uitspraak niet nodig is door beide spelers, namelijk bij politiek risico en bij inflatierisico.

Bij twee risico's voorkeur voor externe accountant

Bij **twee risico's** heeft de **externe accountant** de **voorkeur**. In volgorde van instemming met het doen van een uitspraak betreft dit: **betrouwbaarheid** van de **financiële rapportage** en **financiële risico's** (onder andere disruptie financiële systeem).

Directie

Tabel 2.3.3.4 Belang risico's en wenselijkheid uitspraken internal auditor en externe accountant bij directie

Risico	Directie	≥ 4.5	4 – 4.5		3.5 - 4		3.2 – 3.5		2.8 – 3.2		< 2.8	
	Belang		IA	EA	IA	EA	IA	EA	IA	EA	IA	EA
Markt	4.6									EA	IA	
Informatiebeheer	4.4		IA	EA								
Digitalisering	4.4				IA	EA						
Strategie	4.4					EA	IA					
Handelen in strijd met gedragscode	4.3		IA	EA								
Grote eenmalige projecten	4.1		IA	EA								
Innovatie	4.1						IA			EA		
outsourcing	4.0				IA			EA				
HR	4.0								IA	EA		
Reputatie	4.0					EA	IA					
Politiek risico	3.9								IA	EA		
Regulator	3.9				IA	EA						
Juridisch	3.9					EA	IA					
Day-to-day business	3.8				IA			EA				
Milieu- en klimaat	3.8				IA			EA				
Betrouwbaarheid financiële rapportage	3.7	EA			IA							
Compliance	3.7		IA			EA						
Aansturing interne organisatie	3.7			EA			IA					
Relatiebeheer met derden	3.7					EA	IA					
Financiële risico's (onder andere rente, liquiditeit)	3.6					EA	IA					
Integratie	3.6			EA	IA							
Samenwerking met externe partners	3.4						IA	EA				
Financiële risico's (bijvoorbeeld disruptie financieel systeem)	3.4					EA	IA					
Inkoopmarkt	3.1								IA	EA		
Inflatie	3.1										IA	EA

Legenda
- In de eerste kolom zijn de afzonderlijke risico's genoemd in wat compactere vorm dan in de eerdere paragrafen van dit hoofdstuk.
- In de tweede kolom staat het belang van het risico, zoals aangegeven door de directie in afnemende mate van belang. De (zeer) belangrijke risico's hebben een kleur gekregen.
- In de volgende kolommen staan de gehanteerde klassen weergegeven voor de mate van instemming met een uitspraak door respectievelijk de internal auditor (= IA) en de externe accountant (= EA).

Directie relatieve voorkeur voor externe accountant

Vergeleken met het basisprofiel en de meeste andere benchmarks vertrouwt de **directie relatief meer** op de inbreng van de **externe accountant**.
Bij **tien risico's** heeft de **externe accountant** de **voorkeur.** Bij twee leidt dat zelfs tot een twee klassen hogere mate van instemming, namelijk bij **betrouwbaarheid** van de **financiële rapportage** en **aansturing interne organisatie**. De overige risico's betreffen in volgorde van instemming met het doen van een uitspraak: integratierisico (duidelijk mee eens), strategisch risico, reputatierisico, juridisch risico, relatiebeheer met derden en de beide financiële risico's (elk van de acht risico's 'min of meer mee eens') en bij marktrisico.
Bij **tien risico's** komen internal auditor en externe accountant in **dezelfde klasse** qua instemming. Hiervan heeft er één betrekking op de klasse dat een uitspraak niet nodig is door beide spelers, in casu inflatierisico.

Bij vijf risico's voorkeur voor internal auditor

De **internal auditor** heeft bij **vijf** risico's steeds één **hogere klasse** qua **instemming**.
In volgorde van mate van instemming zijn dit: compliance risico (wet en regelgeving), risico outsourcing, operationeel risico day-to-day business, milieu- en klimaatrisico en innovatierisico.

Bespiegelingen/vragen/kanttekeningen

Wie doet er uitspraken over bepaalde risicogebieden als externe accountant en internal auditor dat niet doen?
Risicogebieden, waarover weinig tot geen instemming bestaat dat of de internal auditor of de externe accountant daarover een uitspraak doen, interesseren ons. Hoe wordt daarmee omgegaan? Doet de verkoop-/marketingafdeling uitspraken over marktrisico? Wordt er gebruik gemaakt van externe studies/dienstverleners? Of wordt dat te duur gevonden? Wie doet er uitspraken over HR-risico en de invulling van de HR-functie in een organisatie? En wie heeft daarvoor de kwaliteiten? Is politiek risico een speeltje van rvb en/of rvc? Innovatie is een veel gehanteerde term, maar wie beoordeelt hoe de rvb en rvc de risico's op dit gebied managen? En hoe vaak vindt er een update plaats van dit en de andere risico's. Kunnen een internal auditor en een externe accountant wat betekenen op deze gebieden. Of zijn de soms lage scores voor deze risicogebieden een indicatie dat commissaris, lid rvb en internal auditor het zelf ook niet helemaal weten. Zitten ze niet wat vast in een oude opvattingen en traditie van kijken naar risico's?

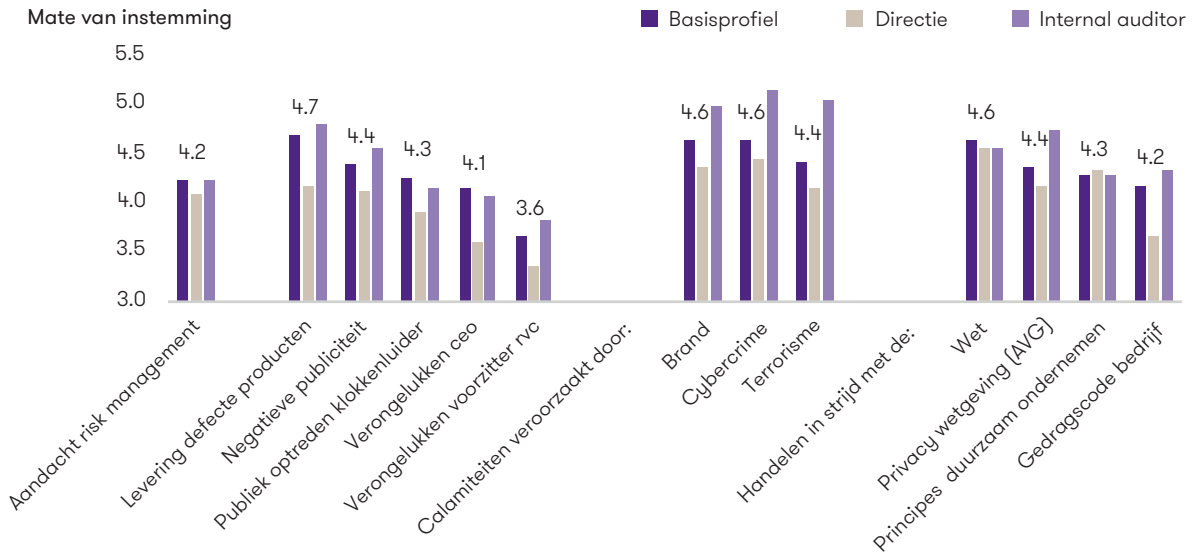
2.4 Calamiteiten en noodscenario's/draaiboeken

Op grond van de boeiende discussies met de verschillende geïnterviewden en na raadpleging van jaarverslagen en andere literatuur is besloten eens een stapje verder te gaan op het onderwerp risicomanagement. Hoe diep ga je als commissaris bij het stellen van de bekende kritische vragen? En als een bestuurder zegt dat het oké is, bent u dan tevreden. En in hoeverre weet u of iets is geregeld of bent u wel eens geconfronteerd met een test? Gebruikt u nog een hotmail account voor uw zakelijk verkeer? Stuurt u berichten naar collega leden rvc, rvb, secretarissen en/of internal auditors inclusief namen, zonder deze te versleutelen? Heeft u zich wel eens afgevraagd in hoeverre u voor het bedrijf het potentiële gat/lek kan zijn met betrekking tot cybercrime?

Bij dit onderdeel hebben we ook de resultaten van een vraag uit het deel relatie 'rvc-rvb' meegenomen. De vraag luidt als volgt: 'de rvc schenkt voldoende aandacht aan risicomanagement'. En ook nu weer de huidige en de gewenste situatie in combinatie met de mate van instemming.

2.4.1 Wenselijkheid van noodscenario's/draaiboeken

Figuur 2. 4 Wenselijkheid van het hebben van noodscenario's/draaiboeken



Voor 92 procent van de calamiteiten is een draaiboek duidelijk wenselijk

Basisprofiel
In de categorie **'beslist mee eens'** (score ≥ 4.5) wat betreft het hebben van een draaiboek/noodscenario vallen: levering **defecte producten**/diensten, calamiteiten veroorzaakt door **brand** en door **cybercrime** alsmede handelen in strijd met de **wet**. **'duidelijk eens'** (4.0 ≤ score mate van instemming < 4.5) met draaiboeken voor alle overige calamiteiten, behalve voor het verongelukken van de voorzitter van de rvc.

In deze beide klassen vallen **elf van de twaalf** onderzochte calamiteiten oftewel **92 procent** van het totaal.
Ook is het basisprofiel het **duidelijk eens** met de stelling dat de **rvc voldoende aandacht** moet schenken aan **risicomanagement**.

Verongelukken voorzitter rvc uitzondering

In de categorie '**min of meer mee eens**' (3.5 ≤ score < 4.0) wordt het draaiboek aangetroffen voor het verongelukken van de voorzitter van de rvc. Daarmee is dit van de onderzochte calamiteiten een opvallende uitzondering.

Gedeeld zijn van wensen voor afzonderlijke noodscenario's met tussen haakjes percentage van het totaal aantal benchmarks

Veel bijval voor draaiboek voor cybercrime, brand, levering defecte producten en handelen in strijd met wet, gedragscode en privacy wetgeving

'**Beslist of duidelijk mee eens**' (score ≥ 4.0) wat betreft het hebben van een draaiboek/noodscenario gaat bij meer dan **80 procent** van de benchmarks op voor: **brand** en **cybercrime** (elk 100), handelen in strijd met de **wet** en in strijd met **privacy** wetgeving (AVG) (elk 94) en levering **defecte producten/diensten** en handelen in strijd met **gedragscode** bedrijf (elk 83).
Lager, **maar** beslist nog **substantieel** in deze categorie is het draagvlak voor de draaiboeken voor **terrorisme** (56), **verongelukken** van de **CEO** en handelen in strijd met de principes van **duurzaam ondernemen** (elk 50). Ook het noodscenario voor publiek optreden van een klokkenluider (44) heeft nog het nodige draagvlak.
Het **draagvlak** voor een draaiboek in verband met het **verongelukken** van de **voorzitter rvc** is met 11 procent **erg laag**. Alleen de commissaris elders lid rvb en de vrouwelijke commissaris zijn duidelijk van mening dat ook in deze situatie een draaiboek wenselijk is. Wanneer ook wordt gekeken naar een klasse lager, dat wil zeggen **'min of meer mee eens'** (score tussen 3.5 en 4.0), dan blijkt voor de meeste genoemde calamiteiten een draaiboek opportuun te zijn. Minder dan 100 procent draagvlak komt dan alleen voor bij terrorisme, verongelukken van de CEO, handelen in strijd met de principes van duurzaam ondernemen (elk 83) en verongelukken van de voorzitter van de rvc (50).
Wat betreft het **voldoende aandacht** hebben als rvc voor **risicomanagement** worden de facto **door alle benchmarks** de opvattingen van het basisprofiel **gedeeld**.

Andere benchmarks vergeleken met het basisprofiel

Bedrijfsgebonden profielen 62 procent, alleen lagere eisen. Persoonsgebonden slechts 32 procent en deels hogere en deels lagere eisen

Bij de **bedrijfsgebonden profielen** is het percentage grote **afwijkingen** van het basisprofiel **62 procent**. De profitsector en de non-profitsector ontlopen hierbij elkaar niet veel. **Alle afwijkingen** betreffen een **lagere** mate van **instemming** bij deze benchmarks dan bij het basisprofiel.
De **persoonsgebonden profielen** laten een wat meer **gedifferentieerd beeld** zien. **Overall** is het percentage grote verschillen **32 procent**, waarvan 25 procent bij de **commissarissen**, 50 procent bij **directie** en **secretaris** en 33 procent bij de **internal auditor**. Bij de directie en de secretaris is er steeds sprake van een negatief verschil (in casu lagere eisen) en bij de internal auditor van een positief verschil. Bij de commissarissen valt op dat de benchmark commissarissen die geen internal audit afdeling hebben, lagere eisen hebben. De **vrouwelijke commissaris** en de **commissaris** elders **lid rvb** hebben juist positieve verschillen (in casu **hogere eisen**).

Bespiegelingen/vragen/kanttekeningen

Hoe zeker weet een lid rvc, lid rvb, secretaris of internal auditor dat er een actueel draaiboek is?

Tijdens de interviews bleek dat menig respondent veronderstelde dat bij een (groot) deel van de gegeven situaties een draaiboek aanwezig was. In al de elf jaar, dat wij nu met het onderzoek bezig zijn, hebben wij nog nooit meegemaakt dat zoveel van de geïnterviewden een aantekening maakte om op dit onderdeel toch nog eens navraag te doen bij de betrokken organisatie. Zekerheid over de feitelijk situaties was bepaald geen gemeengoed. In aanvulling op deze situatie wisten weinig commissarissen zich te herinneren, wanneer voor het laatst over deze invulling van het risk management gesproken was. En wat betreft het weet hebben van een oefening om te zien of de betrokken draaiboeken functioneerde, moesten sommige commissarissen in het verre grijze verleden duiken. Gelukkig is de wereld sinds die tijd niet veranderd!
En om u gerust te stellen, er waren ook diverse leden van rvb's/directies en internal auditors die voor de huidige situatie het antwoord schuldig moesten blijven, omdat ze het niet wisten.
De hiervoor geschetste ervaringen vertaalde zich ook in minder antwoorden bij de huidige situatie dan bij de wenselijke situatie. Bij een viertal beschreven oorzaken van een calamiteit varieerde dat verschil tussen de 5 en

10 procent. Het betrof: verongelukken van CEO en/of voorzitter rvc, terrorisme en het publiek optreden van een klokkenluider.
Kan een commissaris volstaan met een vraag op dit gebied? En als de directie/rvb antwoordt dat dergelijke draaiboeken er zijn, is dan de volgende vraag en wanneer zijn ze voor het laatst getest? En als de directie dan zegt bijvoorbeeld drie jaar geleden, vraagt u dan ook of dit alleen voor het hoofdkantoor is of ook voor de andere vestigingen of voor het samen reizen van 'sleutelfunctionarissen'? En vindt u drie jaar geleden acceptabel? En zijn dit onderwerpen die primair de auditcommissie raken of ook de voltallige rvc?
Een goed voorbeeld van hoe het anders kan, kregen we tijdens onze interviews ook te horen: in een organisatie zijn voor een aantal van deze genoemde draaiboeken vertegenwoordigers benoemd met als taak een jaarlijkse actualisering daarvan te maken en daarover te rapporteren.

Waarom is een draaiboek voor terrorisme niet zo wenselijk?
Deze vraag zou tien jaar geleden bij de meeste bedrijven belachelijk zijn gevonden. Maar is dat nu ook zo? Als we de kranten zien, blijkt ook West-Europa en daarbinnen ook Nederland geen maagdelijk gebied meer te zijn wat betreft ervaring met terrorisme. Stelt u eens voor. Er wordt een brandalarm gegeven. De rvc vergadert net in het hoofdkantoor met de rvb. Iedereen gaat naar buiten. Soms door dezelfde uitgang. Iedereen moet zich verzamelen op een vast punt, bijvoorbeeld een groot plein of weiland met aan drie zijden een groot water van 5 meter breed met aan de binnenkant een 2,5 meter hoge, stevig metalen hek, aan de vierde kant een hoge muur en in die hoge muur een in- en uitgang met elektronische beveiliging en portiers. Geen probleem lijkt het. Maar veronderstel nu eens dat er een bommelding wordt gegeven. Zal dan iedereen ook niet naar buiten gaan naar hetzelfde plein? En stel dat die bommelding alleen maar tot doel had om mogelijke slachtoffers naar buiten te krijgen, zodat terroristen zelf niet naar binnen hoeven te gaan. En stel dat deze over vergelijkbare drones beschikken als gebruikt voor de Saoedische olie-installaties, wat kan er dan gebeuren? De hier geschetste situatie is een compilatie van informatie uit de interviews en uit de media.

Waarom geen draaiboek voor het verongelukken van de voorzitter van de rvc?
Ook bij deze gebeurtenis delen wij wat van onze gedachten met u. Diverse respondenten gaven aan dat bij hun organisatie er wel wat was geregeld, doordat er een vicevoorzitter van de rvc was aangesteld. De vraag is dan of de vicevoorzitter primair geschikt is om tijdelijk de vergadering te leiden en/of ook de lopende gang van zaken te behartigen. Of moet de vicevoorzitter een min of meer volledige remplaçant van de voorzitter kunnen zijn? Vermoedelijk zal de eerste situatie actueler zijn dan de tweede. Maar nu is de voorzitter opeens niet meer beschikbaar. En stel dat er een beslissing moet worden genomen over het verlengen van de zittingstermijn van de CEO, die binnen zes maanden verloopt. De voorzitter van de rvc was niet alleen de linking pin naar de CEO vanuit de rvc, maar had ook het meeste zicht op het functioneren van de CEO. In de selectie- en benoemingscommissie had de voorzitter al een keer geopperd dat een verlenging van de zittingstermijn waarschijnlijk niet zijn voorkeur had. Wel had de voorzitter zijn overwegingen nog niet gedeeld met zijn collega's. Wordt nu de vicevoorzitter belast met de taak van de voorzitter wat betreft het voorbereiden van de beslissing over de verlenging van de termijn van de CEO? Of wordt er eerst kritisch gekeken of een andere lid van de rvc voorzitter moet worden? Of wordt er beslist of er een tijdelijke voorzitter of commissaris van buiten moet komen met ervaring bij dit soort herbenoemingsprocessen? Of toch maar de weg van minste weerstand gekozen en de CEO zijn herbenoeming gegeven? Maar wat zijn de opportunity costs van een keuze voor een verkeerde CEO?
Een tweede voorbeeld, identiek aan het voorgaande wat betreft de vicevoorzitter en de voorzitter. We veronderstellen dat we nu met een beursgenoteerd bedrijf hebben te maken. De CEO problematiek vervalt. Alleen nu staat het bedrijf voor een aantal belangrijke beslissingen op het gebied van digitalisering. De voorzitter was redelijk expert op dit gebied en kende de organisatie goed. Ook had de voorzitter zijn sporen verdiend op M&A-gebied. Nu komt er opeens een private equity partij die een vijandig bod doet op het bedrijf. Wat nu?

2.4.2 Veranderwensen en aanwezigheid van noodscenario's draaiboeken

Tabel 2.4.2 Veranderwens basisprofiel en enige benchmarks

	bapr	MKB	Corp	Zorg	VZ	VR	DIR	IA	Totaal
Aandacht risicomanagement									6
Levering defecte producten									9
Negatieve publiciteit									13
Publiek optreden klokkenluider									16
Verongelukken CEO									17
Verongelukken voorzitter rvc		BP		BP					17
Calamiteiten veroorzaakt door:									
Brand									3
Cybercrime									8
Terrorisme									9
Handelen in strijd met de:									
Wet									5
Privacy wetgeving (AVG)									7
Gedragscode bedrijf									4
Principes duurzaam ondernemen									16

Blanco: de afwijking van het belang ligt tussen de +10 tot en met -10 procent en is in beginsel acceptabel; oranje: de afwijking ligt tussen de -10 tot en met -20 procent en is daarmee beslist een punt van aandacht; rood: de afwijking is onder de -20 procent gelegen, actie is noodzakelijk; totaal: totaal aantal benchmarks met een verander-wens voor het betrokken aandachtsgebied.
BP: Bespreekbaar punt, het ambitieniveau scoort in de wenselijke situatie < 3.2.

Er is voldoende aandacht voor risicomanagement. Wel zes verbeterwensen, waarvan twee urgent

Basisprofiel

Het basisprofiel is het duidelijk eens (score 4.1) met de stelling dat de rvc **voldoende aandacht** moet schenken aan **risicomanagement**. En vindt dat dit ook plaatsvindt. Er is **geen** noodzaak om een **verandering** aan te brengen. Overigens hebben zes van de achttien benchmarks op dit onderdeel wel een **verbeterwens** (33 procent).
Bij zes van de dertien onderdelen heeft het basisprofiel echter een veranderwens. Die voor het hebben van een draaiboek bij het **verongelukken** van de **CEO** (17 keer)[10] en bij het **handelen in strijd** met de principes van **duurzaam ondernemen** (16 keer) zijn **urgent**.
Ook de instemming met het hebben van draaiboeken ten aanzien van levering defecte producten (9 keer), **negatieve publiciteit** (13 keer), **publiek optreden** van een **klokkenluider** (16 keer) en **verongelukken** van de **voorzitter** van de **rvc** (17 keer) indiceert een verbeterwens. Daarbij zij opgemerkt dat die bij het verongelukken van de voorzitter van de rvc als **bespreekbaar punt** worden gekwalificeerd. Hetzelfde geldt ook voor het verongelukken van de CEO bij de **onderwijssector**.
Voor alle benchmarks en het basisprofiel gezamenlijk is het **overall veranderpercentage** 57 **procent.** Dat komt overeen met 124 van de 216 antwoordopties. Dat is aan de forse kant.

Veranderpercentage bedrijfsprofielen 67 procent en persoonsgebonden profielen 48 procent

Veranderwensen bij andere benchmarks

Het overall **veranderpercentage** van de **bedrijfsprofielen** is **67** procent, waarbij de profitsector en de non-profitsector elkaar nauwelijks ontlopen. Bij de **persoonsgebonden profielen** is het overall veranderpercentage **48** procent, waarvan **50** procent bij de **commissarissen** en **44** procent bij de **niet-commissarissen**. Bij deze laatste groep varieert dit van **29** procent bij directie en secretaris tot **75** procent bij de **internal auditor**.

10 Tussen haakjes staat het aantal benchmarks dat bij deze calamiteit/risicogebied een veranderwens heeft, met behalve primair bij het verongelukken van de voorzitter van de rvc, telkens een verbeterwens.

Vijf profielen met veranderpercentage van 75 of meer

Een **veranderpercentage** van **75 procent** of **hoger** komt voor bij de volgende benchmarks: het **familiebedrijf** en de **onderwijssector** (elk 100[11]), de **zorgsector** (92), de **internal auditor** en de **commissaris** bij het **bedrijf zonder internal auditor** (75).
Een veranderpercentage van **50 tot 75 procent** komt voor bij: groot niet-beursgenoteerd bedrijf (67), MKB en 1tier (elk 58) alsmede bij basisprofiel, overige non-profit, commissaris elders lid rvb, de jonge commissaris en de vrouwelijke commissaris (elk 50).

Directie en woningcorporatie laagste veranderpercentage

In de categorie van **25 tot 50 procent** hebben de volgende benchmarks hun veranderpercentage liggen: de **voorzitter** (42), de **commissaris** lid **auditcommissie** en de **secretaris** (elk 33) en **woningcorporatie** en de **directie** (elk 25).
Zowel de voorzitter als de commissaris van de woningcorporatie behoren historisch gezien tot de benchmarks met doorgaans de minste veranderwensen. De lage positie van de directie is wellicht te herleiden tot hun eigen verantwoordelijkheid op deze gebieden. En dan bestaat de neiging deze doorgaans wat rooskleuriger in te vullen dan als dat door een buitenstaander gedaan zou worden.

Veranderwensen per aandachtsgebied

Een derde benchmarks wil meer aandacht voor risicomanagement

Slecht **zes benchmarks** zijn van mening dat er een **verbetering** wenselijk is bij de **aandacht** voor **risicomanagement**. Dit zijn de bedrijfsbenchmarks: groot niet-beursgenoteerd bedrijf, familiebedrijf, zorg- en onderwijssector, overige non-profitbedrijven en de organisaties, waar geen internal auditor is.

Wegvallen CEO en voorzitter rvc meest gedeelde veranderwensen

De **meest gedeelde veranderwensen** bij de achttien benchmarks betreffen de risicogebieden: **verongelukken CEO** en **voorzitter rvc** (elk 17 keer), **publiek optreden** van een **klokkenluider** en **handelen** in **strijd** met de principes van **duurzaam ondernemen** (elk 16 keer) en **negatieve publiciteit** (13 keer).
In de **middenmoot** qua gedeelde veranderwensen komen: **terrorisme** en levering **defecte producten/diensten** (elk 9 keer), **cybercrime** (8 keer) en **handelen in strijd** met **privacy** wetgeving (7 keer).
De andere risicogebieden zijn vijf keer of minder genoemd. Het gaat nu over: brand (3 keer), handelen in strijd met gedragscode (4 keer) en handelen in strijd met de wet (5 keer).

Huidige situatie

Bij vier risicogebieden meer dan 50 procent met draaiboek

In de huidige situatie is slechts **bij** een **viertal risicogebieden** sprake van **50 procent** of meer (≥ 9 keer) benchmarks met een **duidelijke instemming** met de aanwezigheid van een draaiboek. Het gaat dan over: brand (12 keer), cybercrime (10 keer), defecte producten/diensten en handelen in strijd met de gedragscode van het bedrijf (elk 9 keer).
Bij **drie risicogebieden** is dit zelfs **0 procent**, en wel bij verongelukken CEO, voorzitter rvc en handelen in strijd met de principes van duurzaam ondernemen. Ook de 6 procent bij het publiek optreden van een klokkenluider is niet erg indrukwekkend.

11 Het betreft het percentage veranderwensen bij de 12 onderzochte risicogebieden.

Bespiegelingen/vragen/kanttekeningen

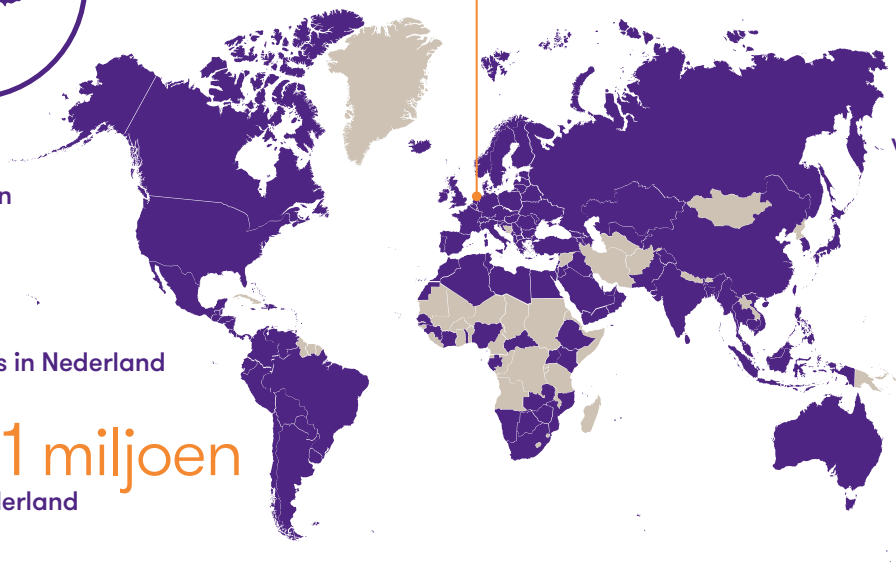
Valt bekendheid met draaiboeken op risicogebieden niet onder de toezichtfunctie van de rvc?
Slechts zes benchmarks zijn van mening dat zij ten aanzien van aandacht voor risicomanagement daaraan meer aandacht moeten besteden. Opvallend is dan dat het veranderpercentage van alle benchmarks gezamenlijk 57 procent is. Dat roept een aantal vragen op. Hoe zeker weet een commissaris dat er op de onderzochte gebieden een draaiboek is? Moet een commissaris dat wel weten of is dit te gedetailleerd? Beperkt de discussie over risicomanagement zich tot de auditcommissie of is het een zaak van de voltallige rvc? In hoeverre wordt met een klassieke oriëntatie gekeken naar risicogebieden en risicomanagement?
En als de commissarissen vinden dat zij voldoende aandacht besteden aan risicomanagement, wat is dan de verklaring voor het hoge veranderpercentage? Betekent dit dan dat voldoende aandacht niets hoeft te zeggen over de kwaliteit van de aandacht? Of is het zo dat de aandacht voldoende is, maar de directie maar niet komt met een bevredigende invulling, oftewel het is nog steeds 'work in progress'?

Hoe kijkt de internal auditor naar risicomanagement en draaiboeken?
Hoe komt het dat de internal auditor (= IA) zoveel veranderwensen heeft? In hoeverre heeft de IA zelf nagedacht om van scratch af aan eens naar het begrip risicomanagement te kijken? En is daarbij dan het bedrijf, het bedrijfsmodel en omgeving, waarin dit bedrijfsmodel moet worden uitgevoerd, ook aan de orde geweest? Of is de IA in de functie gestapt en heeft deze voortgeborduurd op wat er al lag/gebruikelijk was? Of dagen de rvc en rvb de IA onvoldoende uit om buiten zijn (verondersteld) kader te stappen?

Wordt wel eens nagedacht over Murphy's law in casu samenvallen van risico's?
In navolging van de financiële crisis van 2008, waarbij opeens interdependenties bleken te bestaan die de meeste, zo niet bijna alle, organisaties zich niet hadden gerealiseerd, vragen wij ons af in hoeverre interdependenties tussen de afzonderlijke risicogebieden wel eens en ook voldoende aandacht krijgen. Laten we eens een fictief voorbeeld nemen. Per 1 januari 2021 treedt er een nieuwe wet in werking, waardoor bijvoorbeeld banken, nutsbedrijven, woningcorporaties en verzekeraars aan gemeenten moeten melden dat er bewoners zijn met betalingsachterstanden. De volgende vragen dienen zich aan: zijn de genoemde organisaties in staat deze informatie aan te leveren? Wat kost het deze organisaties om aan deze verplichting te voldoen? Welke sancties staan er op het niet goed nakomen van deze verplichting? En wat is 'goed'? Hoe verhoudt deze meldingsplicht zich met de wet op de privacy? Stel dat dit strijdig is, wie krijgt dan een boete? En vragen richting gemeenten. Zijn de gemeenten toegerust om deze meldingen te verwerken? Welk beslag legt dit op het gemeentelijk apparaat? Wie neemt de extra budgettaire lasten voor zijn rekening? Vast niet de centrale overheid. En kan of moet een gemeente in zee gaan met vrijwilligers organisaties en/of professionele partijen om follow up te geven? Stel dat dit systeem wordt ingevoerd en aannemende dat het op de langere termijn bijdraagt tot het eerder signaleren van mensen, die mogelijk in financiële problemen komen. Dan is het aannemelijk dat er in macrotermen gezien een besparing optreedt. Alleen wie neemt de voorfinanciering voor zijn rekening? En als dit noodzaakt tot het al dan niet tijdelijk aantrekken van extra mensen, waar zijn die te vinden? Toch niet uit de arbeidsruif, waar ook de extra agenten, de extra leraren en het extra zorgpersoneel vandaan moet komen? En wat als de overheid opeens beslist dat de aanpak van de hier geschetste problematiek de maatschappelijke taak is/wordt van de bedrijven/werkgevers?

Maak kennis met Grant Thornton

730+
vestigingen wereldwijd



$ 5,72 miljard
wereldwijde omzet

9
vestigingen in Nederland

56.000+
professionals wereldwijd

550+
medewerkers in Nederland

meer dan 140 landen

€ 63,1 miljoen
omzet in Nederland

Grant Thornton
An instinct for growth™

www.gt.nl

Grant Thornton Accountants en Adviseurs B.V. is lid van Grant Thornton International Ltd. (Grant Thornton International). Grant Thornton International en haar leden zijn geen wereldwijde vennootschap. Diensten worden geleverd door de onafhankelijke leden.