Vertrouwen in de kwetsbare keten

Publieke managementletter over ketenrisico's, afhankelijkheden en bestuurlijke weerbaarheid.

Koninklijke Nederlandse Beroepsorganisatie van Accountants

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Instituut van Internal Auditors Nederland

Februari 2026

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Instituut van
Internal Auditors
Nederland

Nederland rekent op zijn accountants, IT-auditors en internal auditors.

De Koninklijke NBA helpt accountants hun cruciale rol in de maatschappij te vervullen, nu en in de toekomst. De leden van de Koninklijke NBA vormen een brede, pluriforme beroepsgroep van ruim 22.000 professionals werkzaam in de openbare accountantspraktijk, bij de overheid, als intern accountant en in het management van organisaties. Integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag zijn essentiële waarden voor iedere accountant.

NOREA vertegenwoordigt bijna 1.700 Register IT-auditors (RE's) die onafhankelijk oordelen over de betrouwbaarheid, veiligheid en continuïteit van digitale systemen en data. In een economie die sterk leunt op technologie en online dienstverlening helpen deze IT-auditors organisaties en maatschappij om digitale risico's te beheersen en vertrouwen in de keten te versterken. Register IT-auditors (RE's) zijn hoog opgeleid (post-master) en werken volgens strikte beroeps- en gedragsregels. NOREA ziet toe op kwaliteit en ondersteunt IT-auditors in hun cruciale maatschappelijke rol.

Instituut van Internal Auditors Nederland (IIA Nederland) is de beroepsorganisatie voor Internal Auditors in Nederland en vertegenwoordigt ruim 3.000 professionals werkzaam in zowel de publieke als private sector. Internal Auditors ondersteunen bestuur en toezichthouders bij het realiseren van strategische doelstellingen, het beheersen van risico's en het versterken van governance door middel van onafhankelijke en objectieve assurance en advies vanuit de organisatie zelf. IIA Nederland maakt deel uit van het wereldwijde Institute of Internal Auditors (IIA) en verbindt internationale standaarden en inzichten met de Nederlandse praktijk. Door het bevorderen van vakmanschap, objectiviteit en kwaliteit draagt IIA Nederland bij aan transparant, verantwoord en weerbaar bestuur.

Dit document bevat bladwijzers, hyperlinks en navigatiebuttons

 Adobe Acrobat bladwijzers - toetsencombinatie “Ctrl-b”

Tekst is een interne document- of externe hyperlink

Naar inhoudsopgave

Vorige pagina

Volgende pagina

Bestuurders, toezichthouders, accountants, IT-auditors, internal auditors
en andere belanghebbenden,

Postbus 242
2130 AE Hoofddorp
Mercuriusplein 3
2132 HA Hoofddorp
T 088 4960 301
nba@nba.nl
www.nba.nl

De afgelopen jaren is duidelijk geworden hoe kwetsbaar onze economie is geworden door verweven digitale, logistieke en datagedreven ketens. Verstoring bij één partij – of dat nu een cloudprovider, producent van kritieke componenten, logistiek knooppunt of datadienstverlener is – kan zich binnen luttele uren verspreiden naar talloze organisaties. De realiteit van vandaag is dat continuïteit niet meer binnen de muren van de eigen organisatie wordt bepaald, maar in ketens die alsmaar complexer, internationaler en moeilijker te overzien zijn.

Deze kwetsbaarheid wordt vergroot door geopolitieke spanningen, de afhankelijkheid van enkele mondiale technologie- en IT-leveranciers, nieuwe Europese kaders (zoals Digital Operational Resilience Act (DORA), Network and Information Security Directive (NIS2) en de Corporate Sustainability Reporting Directive (CSRD) en de groeiende maatschappelijke druk op transparantie. Incidenten versterken elkaar, risico's stapelen zich op buiten het directe zicht van bestuurders, en governance-instrumenten die jarenlang volstonden, blijken onvoldoende toegerust voor deze samenhangende risico's.

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

In deze gezamenlijke Publieke managementletter (PML) van de NBA-Signaleringsraad, NOREA en IIA Nederland staat één vraag centraal: hoe houden bestuurders, accountants, IT-auditors en internal auditors gezamenlijk grip op ketens waarin zekerheden verschuiven?

Wij signaleren dat dit vraagt om nieuw inzicht, een open gesprek en andere manier van samenwerken. Organisaties moeten niet alleen weten *wie* hun kritieke leveranciers zijn, maar ook *hoe* processen, data en verantwoordelijkheden door ketens heen bewegen – en *wat* dat betekent voor continuïteit, veiligheid en maatschappelijke verantwoordelijkheid.

Die beweging geldt ook voor onze beroepsgroepen. De werkzaamheden van accountants, IT-auditors en internal auditors zijn in de praktijk uit elkaar gegroeid, terwijl moderne ketenrisico's juist vragen om nauwere verbinding. Bestuurders verwachten duidelijkheid over afhankelijkheden, aannames en grenzen van assurance, zowel vanuit de organisatie zelf als vanuit onafhankelijke externe toetsing. Dat vraagt om disciplines die elkaar versterken, elkaars inzichten verbinden en gezamenlijk bijdragen aan een integraal risicobeeld.

Deze Publieke managementletter *Vertrouwen in de kwetsbare keten* bevat zes signalen over de kwetsbaarheid van moderne ketens, de grenzen van assurance, de noodzaak van integraal ketenzicht en de rolvernieuwing binnen onze beroepsgroepen. De eerste vijf signalen zijn gericht op bestuurders en toezichthouders om ketenweerbaarheid binnen de organisatie te versterken. Het zesde signaal richt zich expliciet op accountants en IT-auditors en doet een appèl op het beroep om waarde toe te voegen waar onzekerheden het grootst zijn.

Het versterken van ketenvertrouwen is geen technische exercitie, maar een gezamenlijke verantwoordelijkheid. Bestuurders, toezichthouders, accountants, IT-auditors en internal auditors hebben elkaar daarbij nodig. Met deze gezamenlijke PML willen de NBA-Signaleringsraad, NOREA en IIA Nederland dat gesprek versterken en versnellen.

Hoogachtend,

Leen Paape
Voorzitter NBA-Signaleringsraad

Marc Welters
Voorzitter NOREA

Frans Eusman
Voorzitter IIA Nederland

Inhoudsopgave

Samenvatting

Organisaties leunen steeds sterker op complexe ketens van leveranciers, datadiensten en digitale platforms. Daardoor kan één verstoring direct gevolgen hebben voor continuïteit en bestuurlijke besluitvorming. Nieuwe kaders zoals DORA, NIS2 en CSRD versterken de verplichting voor bestuurders om inzicht te hebben in strategische afhankelijkheden, dataflows en digitale weerbaarheid.

Assurance blijft waardevol, maar dekt slechts een deel van deze werkelijkheid. Rapporten laten zien dat processen in een periode hebben gewerkt zoals bedoeld, maar bieden geen garantie dat ketens functioneren bij verstoringen of dat onderaannemers en daarmee de hele keten beheerst zijn. Bestuurders moeten expliciet maken hoe zij afhankelijkheden begrijpen, monitoren en bespreken – en helder zijn over onzekerheden die niet volledig in te schatten zijn.

Dit vraagt om een beter samenspel tussen bestuurders, commissarissen, accountants, IT-auditors en internal auditors. Vertrouwen in de keten ontstaat door gedeeld inzicht, transparantie en samenwerking. Daarom worden in deze Publieke managementletter zes signalen gedeeld die laten zien waar ketenvertrouwen kwetsbaar wordt en welke stappen bestuurders, accountants, IT-auditors én internal auditors kunnen zetten:

1. Verwevenheid vergroot kwetsbaarheid
   Ketens worden langer en ondoorzichtiger - inzicht in leveranciers én onderaannemers is een randvoorwaarde voor continuïteit.

2. Assurance is geen garantie
   Rapporten geven zekerheid over een afgebakende scope en periode, maar vervangen nooit het bestuurlijk oordeel over ketenrisico's.

3. Nieuwe kaders, nieuwe verantwoordelijkheden
   DORA, NIS2 en duurzaamheidseisen maken digitale weerbaarheid en datakwaliteit een expliciete verantwoordelijkheid van bestuur én commissarissen.

4. Weerbaarheid is een bestuursverantwoordelijkheid
   De vraag is niet óf een verstoring plaatsvindt, maar hoe snel organisaties herstellen en hoe goed dat vooraf is georganiseerd.

5. De auditor als verbinder van vertrouwen
   Waarde ontstaat wanneer accountant, IT-auditor en internal audit signalen delen en bestuurders helpen onzekerheden bespreekbaar te maken.

6. Auditdisciplines in beweging: samenwerken aan ketenzekerheid
   Geen enkele discipline overziet de hele keten alleen – samenwerking is nodig om een compleet risicobeeld te leveren.

Inleiding

De realiteit dringt zich op

De afhankelijkheid van ketens bepaalt in toenemende mate de weerbaarheid van organisaties. Een verstoring bij één schakel - of dat nu een leverancier, cloudprovider, logistieke partner, producent van essentiële componenten of datadienstverlener is - kan zich tegenwoordig razendsnel door waardeketens verplaatsen. Daarmee raakt ketenafhankelijkheid direct aan de bestuurlijke opdracht om continuïteit en digitale weerbaarheid te waarborgen.

Toezichthouders AFM en DNB waarschuwden recent in hun gezamenlijke analyse 'Digitale afhankelijkheid in de financiële sector (2025)'[1] dat Nederlandse organisaties, met name in de financiële sector, sterk leunen op een beperkte groep mondiale IT- en cloudaanbieders. Die concentratie creëert een nieuw type kwetsbaarheid: het risico dat één incident een breed maatschappelijk effect veroorzaakt. Dit beeld zien we in vrijwel alle sectoren terug, van industrie tot zorg, van energie-infrastructuur tot digitale dienstverlening.

Daarbovenop komen geopolitieke spanningen, verstoringen in logistieke ketens, druk op grondstoffen en toenemende eisen rond duurzaamheid en maatschappelijke verantwoordelijkheid. Incidenten staan niet meer op zichzelf; ze versterken elkaar. Bestuurders opereren in een omgeving waarin risico's sneller veranderen dan veel van de traditionele governance-instrumenten kunnen bijbenen.

Daarnaast blijft - wettelijk[2] en feitelijk - dat Raad van Bestuur (RvB) en toezicht (Raad van Commissarissen (RvC) / Raad van Toezicht (RvT)) verantwoordelijk zijn voor een adequate organisatie van processen, beheersing en continuïteit. Ook wanneer cruciale processen zijn uitbesteed, kan deze verantwoordelijkheid niet worden gedelegeerd. Dit geldt nadrukkelijk ook voor IT-beheersing: RvB én RvC/RvT moeten periodiek inzicht krijgen in de werking van kritieke processen, systemen en ketenafhankelijkheden.

Vertrouwen in de keten is daardoor geen vanzelfsprekendheid meer - het is een prestatie. Een prestatie die begint met inzicht in afhankelijkheden, helderheid over wat niet volledig beheersbaar is en samenwerking met de partijen waarop organisaties direct en indirect steunen.

Dit vraagt iets van organisaties, waar ook accountants in business dagelijks met deze vraagstukken werken, én van de auditdisciplines. Accountants, IT-auditors en internal auditors zien dagelijks hoe processen, systemen, data, leveranciers en mensen verweven zijn geraakt. Zij constateren dat goed bestuur niet alleen draait om interne beheersing, maar ook om het kennen en beoordelen van de keten waar de organisatie onderdeel van is, inclusief de onzekerheden die zich niet laten wegregelen.

---

1 AFM en DNB waarschuwen voor systeemrisico's financiële sector door digitale afhankelijkheid | De Nederlandsche Bank

2 BW2 art. 2:393 lid 4 verplicht de accountant om te rapporteren over bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking voor zover deze tijdens de controle zijn geconstateerd.
DORA art. 5 en NIS2 art. 20 leggen de eindverantwoordelijkheid voor governance en beheersing van digitale risico's bij bestuur en toezicht, inclusief periodieke rapportage over IT-continuïteit en cyberweerbaarheid. Deze verantwoordelijkheid blijft óók bij uitbesteding bestaan.

De introductie van de Verklaring omtrent Risicobeheersing (VoR) binnen de Corporate Governance Code[3] bevestigt deze beweging: niet alle risico's zijn te voorkomen, maar bestuurders moeten wel expliciet en transparant maken hoe zij afhankelijkheden onderkennen, monitoren en adresseren. Dat raakt de kern van vertrouwen: niet de illusie van volledige zekerheid, maar de kwaliteit van inzicht, dialoog en herstelvermogen.

> Vertrouwen in de keten ontstaat niet door méér rapporten, maar door gedeeld inzicht, in de operationele keten zelf: de leveranciers, systemen, datastromen en partners waarop organisaties dagelijks steunen. Dat vraagt om een eerlijk gesprek over kwetsbaarheden en samenwerking over disciplines en organisaties heen. Alleen wanneer bestuurders, accountants, IT-auditors en internal auditors elkaar vinden, wordt assurance betekenisvol in het licht van die bredere uitbestedings- en afhankelijkheidsketen.

Daarom is deze Publieke managementletter een uitnodiging - zowel aan bestuurders als aan het beroep van accountants, IT-auditors en internal auditors zelf. Aan bestuurders: wees expliciet over uw afhankelijkheden, kwetsbaarheden en herstelvermogen. Aan accountants, IT-auditors en internal auditors: werk samen, maak reikwijdte, aannames en beperkingen zichtbaar, en ondersteun bestuurders bij het voeren van het juiste gesprek - niet door zekerheid te suggereren waar die niet bestaat, maar door duidelijkheid te bieden over wat wél kan.

In de volgende signalen delen we wat wij - als accountants, IT-auditors en internal auditors - in de praktijk zien: waar het mis kan gaan, waar vertrouwen te snel wordt verondersteld en welke stappen bestuurders én het beroep nú kunnen zetten om hun organisatie en hun keten sterker te maken.

Wie geen zicht heeft op zijn keten, heeft ook geen grip op zijn effectiviteit en continuïteit.

3 Corporate Governance Code 2025 | Monitoring Commissie Corporate Governance (mccg.nl)

Signaal 1 |
Verwevenheid vergroot kwetsbaarheid

Vertrouwen in de keten begint niet bij rapporten, maar bij inzicht. Bestuurders moeten weten op wie zij rekenen, wat er gebeurt als een (kritische) schakel uitvalt, en hoe ogenschijnlijk operationele afhankelijkheden kunnen uitgroeien tot strategische risico's.

Organisaties opereren steeds meer in ketens van leveranciers, platforms, datadiensten en onderaannemers. Die verwevenheid maakt sneller én slimmer werken mogelijk, maar vergroot ook de kwetsbaarheid: één verstoring kan productie, dienstverlening en de continuïteit van organisaties raken, met directe gevolgen voor burgers en bedrijven die op deze ketens vertrouwen.

Dat zien we in de praktijk regelmatig gebeuren. De 'kaashack' in 2021 liet zien hoe een ransomware-aanval bij één logistiek dienstverlener tijdelijk leidde tot lege kaasschappen bij Albert Heijn[4]. Het ingrijpen van het kabinet bij chipmaker Nexperia maakte zichtbaar hoe afhankelijk productie- en innovatiesystemen zijn van geopolitieke besluitvorming en van een beperkt aantal leveranciers van kritieke componenten[5]. Ook binnen financiële instellingen blijkt uit toezicht dat uitbesteding aan ICT-dienstverleners steeds complexer wordt: meerdere lagen van onderaannemers, grensoverschrijdende dienstverleningen en contractketens die niet altijd volledig zichtbaar zijn.

Deze verwevenheid betekent dat risico's zich ophopen op plekken waar bestuurders ze niet altijd herkennen. Veel boards hebben geen volledig beeld van:

- welke leveranciers écht cruciaal zijn;
- welke onderaannemers "in de schaduw" meedraaien;
- waar concentratierisico's ontstaan;
- en hoe afhankelijkheden zich verhouden tot nieuwe eisen uit DORA, NIS2 (zie kader op pagina 17) en maatschappelijke verwachtingen.

Contracten blijken in de praktijk vaak verouderd, niet qua datum maar omdat ze geen rekening houden met recente risico's zoals cyberdreigingen, nieuwe wetgeving of internationale leveringsrisico's. In uitbestedingstrajecten ligt de nadruk bovendien veelal op de geleverde diensten, terwijl afspraken over risicobeheersing, compliance en continuïteit juist bepalend zijn voor betrouwbaarheid in de keten.

Zelfs wanneer leveranciers beschikken over gangbare rapporten, zoals ISAE 3402, SOC 2 of ISO 27001 (kader pagina 14), biedt dat geen garantie op ketencontinuïteit. Die rapporten dekken slechts een afgebakende scope; strategische afhankelijkheden, onderaannemers en nieuwe dreigingen blijven daarbij vaak buiten beeld. Meer hierover in Signaal 2: Assurance is geen garantie.

Goed bestuur vraagt daarom om ketenbewustzijn: zien waar de kwetsbaarheden zitten, begrijpen welke afhankelijkheden domineren en weten welke alternatieven of exitscenario's beschikbaar zijn, ook als die beperkt zijn.

4 'Kaas-hack' opgelost, ging om gijzelsoftware (nos.nl)
5 'Problemen Volkswagen door tekort Nexperia-chips, vanavond Duits crisisoverleg (nos.nl)'

Welke acties dienen bestuurders hiervoor binnen hun organisatie uit te zetten en zijn voor de commissarissen aandachtspunten van belang om toezicht op te houden:

- Vraag jaarlijks om een actueel overzicht van kritieke leveranciers en onderaannemers, inclusief afhankelijkheden en ketenrelaties.

- Toets contracten op right-to-audit-clausules, continuïteitsafspraken (zoals fall-back-opties) en exit-mogelijkheden, en actualiseer deze bij wijzigingen in risico's of wetgeving.

- Beoordeel assurance-rapportages kritisch, met oog voor scope, carve-outs en user controls (zie ook kader pagina 15) en gebruik de accountant, IT-auditor of internal auditor om de bevindingen te duiden, maar niet als vervanger van uw eigen oordeel.

- Benut internal audit om ketenbeheersing te toetsen: laat internal audit gericht onderzoeken waar afhankelijkheden, control gaps of knelpunten ontstaan en hoe deze de continuïteit van de organisatie raken.

- Onderzoek concentratierisico's en afhankelijkheid van dominante leveranciers, en stimuleer alternatieven waar dit strategisch wenselijk is.

- Voer scenario-oefeningen uit waarin uitval van een leverancier of datadienst realistisch wordt getest.

Ketenvertrouwen begint bij inzicht: weten op wie u kunt rekenen, waar de kwetsbaarheden zitten en welke handelingsruimte u houdt wanneer één schakel faalt.

Signaal 2 |

Assurance is geen garantie

Zekerheid op papier vervangt geen verantwoordelijkheid in de praktijk. Assurance is het sluitstuk van een bredere dialoog: contracteren, monitoren, samenwerken en pas dan toetsen. Rapporten helpen, maar alleen als bestuurders begrijpen wat eronder ligt.

Bestuurders vertrouwen vaak op ISAE 3402-rapporten, SOC 2-verklaringen of ISO-certificaten als bewijs dat hun leveranciers “op orde” zijn. Maar dat vertrouwen heeft grenzen. Assurance geeft ‘slechts’ zekerheid over een afgebakend deel van de werkelijkheid en over een specifieke periode, niet over de keten als geheel. In een tijd waarin risico’s zich sneller ontwikkelen dan assurance-instrumenten kunnen bijhouden, ontstaat een steeds grotere mismatch tussen wat bestuurders willen weten en wat assurance daadwerkelijk kan leveren.

Assurance-rapportages bevestigen dat bepaalde processen, in een specifieke periode, hebben gefunctioneerd volgens vooraf vastgestelde criteria.
Maar zij zeggen niets over:

- risico’s en onzekerheden die buiten de scope vallen;
- impact van carve-outs waarbij essentiële (sub) dienstverleners buiten beeld blijven;
- ontbrekende of onvolledige user controls binnen de eigen organisatie;
- nieuwe dreigingen die na de rapportageperiode ontstaan;
- strategische afhankelijkheden die een structureel risico vormen, los van proceskwaliteit.

Externe assurance-opdrachten worden uitgevoerd door accountants (RA) of IT-auditors (RE) en zijn gericht op het maatschappelijke verkeer. Internal audit verschaft interne assurance aan het bestuur en management over de opzet en werking van governance, risicobeheersing en interne beheersing binnen de organisatie. In lijn met de Global Internal Audit Standards (GIAS) is afstemming tussen internal audit, accountant en IT-auditor essentieel om hiaten in de dekking van risico’s te voorkomen en dubbel werk te vermijden. ISO-certificering betreft een onafhankelijke toetsing van het bestaan en functioneren van een managementsysteem door certificerende instellingen. Dit verschilt van assurance-opdrachten, waarin auditors een onafhankelijk oordeel geven over specifieke processen of beheersingsmaatregelen binnen een afgebakende scope en periode. Zie ook kader “Welke standaarden geven zekerheid in de keten?” (pagina 14).

In de praktijk zien we dat bestuurders soms méér verwachten dan dat deze instrumenten kunnen waarmaken. De wereld verandert sneller dan de standaarden waarop assurance is gebaseerd. Cloudketens worden langer, AI-systemen complexer, regelgeving zwaarder en onderaannemers talrijker. Tegelijkertijd hebben de beroepsgroepen - accountants én IT-auditors - de afgelopen jaren steeds meer nadruk gelegd op dossiervorming en toetsbaarheid en is de natuurlijke adviesfunctie versmald. Daardoor ontstaat het risico dat bestuurders aannames doen over zekerheid die niet door de assurance kan worden afgedekt.
Assurance is waardevol, maar bestuurders verwachten in de praktijk soms méér zekerheid dan een extern assurance-rapport kan bieden. Het is daarom essentieel te begrijpen wat assurance precies wél en níet

doet en hoe dit zich verhoudt tot ketenrisico's, het functioneren van de organisatie bij verstoringen en strategische afhankelijkheden.

- Assurance geeft een betrouwbaar beeld van het verleden, maar geen garantie voor de toekomst. Rapporten laten zien dat processen in een onderzochte periode hebben gewerkt zoals bedoeld. Maar de werkelijkheid kan door systeemupdates, configuratiewijzigingen, cyberdreigingen of geopolitieke ontwikkelingen snel veranderen.

- Assurance wordt altijd achteraf gegeven, risico's kunnen zich tussentijds al hebben ontwikkeld en buiten de scope van de assurance-rapportage vallen. Tussen het einde van de onderzochte periode en het moment van rapportage kunnen nieuwe kwetsbaarheden ontstaan. Dat maakt assurance nuttig, maar nooit afdoende als enige basis voor bestuurlijke besluitvorming.

- Assurance toetst elementen van een proces, niet de volledige keten. Rapporten richten zich op specifieke systemen of controles binnen een afgebakende scope. Ze dekken geen onderaannemers, concentratierisico's, cloudketens of afhankelijkheden af die buiten de scope vallen.

- Transparantie over continuïteit is een expliciete verantwoordelijkheid van bestuurders. ISAE 3402-rapporten kijken terug, sommige ISAE 3000-rapporten bevatten wel een beperkte forward-looking component, maar kunnen nooit garanderen dat processen of leveranciers in de toekomst blijven functioneren. Wat bestuurders wel moeten doen, is helder zijn over aannames, risico's en onzekerheden rond operationele, digitale, en financiële continuïteit en de impact daarvan op de organisatie en haar omgeving. Assurance ondersteunt dit inzicht, maar vervangt het nooit.

Assurance is een waardevol instrument, maar toont dus nooit het volledige risicobeeld. Het vergroot vertrouwen waar dat kan, maar het neemt onzekerheid niet altijd weg en vervangt de eigen risicobeoordeling niet.

Daarom presenteren we aan het einde van dit signaal een overzicht van de belangrijkste assurance-standaarden die bestuurders in de praktijk tegenkomen, inclusief hun reikwijdte. In het daaropvolgende kader maken wij expliciet wat assurance wél en niet afdekt en welke aanvullende verantwoordelijkheden bij bestuurders horen om ketenzekerheid te borgen.

Goed bestuur vraagt dat bestuurders zelf deze beperkingen van assurance onderkennen, expliciet maken welke risico's buiten beeld blijven en het gesprek voeren met accountant, IT-auditor en internal audit. Assurance ondersteunt het vertrouwen, maar vervangt het bestuurlijke oordeel niet.

Welke acties dienen bestuurders hiervoor binnen hun organisatie uit te zetten en zijn voor de commissarissen aandachtspunten van belang om toezicht op te houden:

- Zie assurance als hulpmiddel, niet als eindpunt. Gebruik het als input voor de dialoog en niet als afvinklijst.
- Weet welke assurance-afspraken met cruciale dienstverleners zijn gemaakt.
- Lees rapporten kritisch, met aandacht voor de grenzen: scope, periode, carve-outs, onderaannemers en user controls.
- Vraag om samenhang: hoe verhouden financiële, digitale en duurzaamheids-assurance zich tot elkaar?
- Gebruik bevindingen uit assurance-rapporten actief: bespreek afwijkingen, kwetsbaarheden en afhankelijkheden met leveranciers en leg vervolgafspraken vast. Laat de belangrijkste bevindingen uit assurance-rapporten onderdeel zijn van interne rapportages.
- Wees expliciet over verwachtingen richting accountant en IT-auditor: zij geven zekerheid over processen, maar leveren geen garantie over strategische keten-continuïteit.
- Gebruik internal audit om het geheel van interne en externe 'assurance'-providers in kaart te brengen en de efficiency (geen dubbel werk!) en effectiviteit daarvan te beoordelen.

Assurance ondersteunt vertrouwen; maar alleen als bestuurders begrijpen hoe dit hun verantwoordelijkheid in de gehele keten ondersteund.

Welke standaarden geven zekerheid* in de keten?

Standaard of norm	*Waar geeft het zekerheid over*	*Wat bestuurders moeten weten*
NV COS ISAE 3402 / NOREA-Richtlijn 3402	Interne beheersing bij uitbesteding van processen die van invloed zijn op de financiële verslaggeving van klanten.	ISAE wordt uitsluitend uitgevoerd door een accountant of IT-auditor RA of RE), handelend binnen de beroeps- en kwaliteitskaders van de NBA of NOREA. Richt zich op de opzet en werking van interne beheersingsmaatregelen bij de dienstverlener. De verklaring dekt uitsluitend de beschreven processen en periode. Let op scope, carve-outs en user controls.
SOC 2 (ISAE 3000 / Richtlijn 3000A – NOREA)	Beheersing rond beveiliging, beschikbaarheid, vertrouwelijkheid, integriteit van processen en privacy van data en systemen.	SOC 2 is geen aparte standaard, maar een rapportvorm onder ISAE 3000 / Richtlijn 3000A, met de structuur van ISAE 3402 en gebruik van de Trust Services Criteria als beheersings-doelstellingen. Gericht op IT-dienstverleners en cloudproviders; ziet niet op het hele bedrijf maar op geselecteerde processen.
ISO 27001	Certificering van het informatiebeveiligings-managementsysteem (ISMS).	Gaat niet over assurance maar over naleving van een managementsysteem. Let op: alleen certificaten die zijn afgegeven door instellingen die zijn geaccrediteerd door de Raad voor Accreditatie (RvA) hebben echte waarde.
NV COS 3810N / ISSA 5000	Assurance over duurzaamheidsinformatie (zoals milieu-, sociale en governance-aspecten).	NV COS 3810N is de huidige Nederlandse standaard; ISSA 5000 wordt de nieuwe internationale norm. Beide stellen eisen aan betrouwbaarheid van data in de hele waardeketen.
DORA / NIS2	Europese kaders voor digitale weerbaarheid en leveranciersbeheer.	Geen assurance-standaarden, maar wettelijke verplichtingen voor ketenverantwoordelijkheid: organisaties moeten hun uitbestedingsketen volledig in kaart brengen en het bestuur blijft eindverantwoordelijk voor de beheersing en continuïteit.

Samenvatting voor bestuurders

Assurance-rapporten tonen aan dat processen effectief functioneren binnen een afgebakende scope. Certificaten laten zien dat een managementsysteem formeel aanwezig is. Geen enkel rapport vervangt echter het eigen oordeel: bestuurders moeten weten wie de zekerheid afgeeft, wat eronder valt en welke risico's buiten beeld blijven.

Deze standaarden en rapportages bieden daarmee een eerste vorm van zekerheid – een belangrijk vertrekpunt, maar nooit de volledige werkelijkheid. In het volgende signaal gaan we in op wat dat betekent voor bestuurders en toezichthouders: waarom assurance geen garantie is, en waar de eigen verantwoordelijkheid begint.

*) *NB: Assurance-rapporten verschillen in de mate van zekerheid die zij bieden. Sommige geven een redelijke mate van zekerheid (meer uitgebreid onderzoek), andere een beperkte mate van zekerheid (beoordeling op hoofdlijnen). Het rapport zelf vermeldt altijd welke vorm van zekerheid wordt verstrekt.*

Keten-assurance in perspectief

Wat een assurance- of certificeringsrapport wél doet	*Wat bestuurders aanvullend moeten borgen*
Geeft zekerheid over een afgebakend proces, systeem of periode – niet over de gehele organisatie of keten.	Vraag expliciet naar de scope van het onderzoek en welke onderdelen buiten beschouwing zijn gelaten (carve-outs). Overweeg wat dat betekent voor uw eigen risico's en continuïteit.
Baseert zich op vooraf vastgestelde criteria, maar de herkomst daarvan verschilt per standaard. Bij ISAE 3402 stelt de dienstverlener zelf de controle-doelstellingen vast; bij SOC 2 zijn de Trust Services Criteria voorgeschreven; bij ISO 27001 worden de eisen bepaald door de norm en het toepassingsgebied van het ISMS.	Begrijp welke criteria zijn gebruikt en wie ze heeft vastgesteld. Toets of deze aansluiten bij uw eigen risicobeeld en informatiebehoefte. Overweeg – eventueel met branchegenoten – invloed uit te oefenen op de gekozen normen of scope.
Verwacht dat u als afnemer user controls uitvoert om de ketenbeheersing sluitend te maken. Dit zijn beheersmaatregelen binnen uw eigen organisatie (mede bedoeld om de uitbesteding goed te laten functioneren).	Richt deze user controls daadwerkelijk in – denk aan toegangsbeheer, incidentafhandeling en verificatie van rapportages van de leverancier – en leg deze aantoonbaar vast voor audit en toezicht.
Wordt uitgevoerd als assurance (zoals ISAE 3402, ISAE 3000 of ISSA 5000) of als certificering (zoals ISO 27001), elk met eigen kwaliteitsborging. Bij assurance-opdrachten gelden de professionele kaders van NBA en NOREA; bij certificering is de auditor soms geaccrediteerd (bijv. via de Raad voor Accreditatie (RvA)), maar dat is niet verplicht.	Verifieer bij certificering altijd of de certificeerder RvA-geaccrediteerd is en beoordeel de scope en reikwijdte van het certificaat. Vertrouw op de professionele kaders, maar blijf kritisch: een positief rapport ontslaat bestuurders niet van hun eigen verantwoordelijkheid.
Richt zich doorgaans op één organisatie, terwijl risico's vaak ontstaan in onderaannemingen en ketenpartners buiten beeld.	Vraag of en hoe de leverancier toezicht houdt op zijn eigen keten. Overweeg gezamenlijke audits of sectorale afspraken om ketenrisico's beter te beheersen.

Wat een assurance- of certificeringsrapport niet doet	*Wat bestuurders aanvullend moeten borgen*
User controls: Het rapport benoemt welke beheersmaatregelen de afnemer zelf moet uitvoeren om de ketenbeheersing sluitend te maken. Deze user controls vallen buiten het onderzoek.	Controleer of deze maatregelen binnen de eigen organisatie daadwerkelijk zijn ingericht en functioneren, en leg vast wie daarvoor verantwoordelijk is.
Carve-outs: Delen van de dienstverlening, systemen of leveranciers kunnen buiten de scope van het onderzoek vallen.	Lees het rapport kritisch: over uitgesloten onderdelen is geen zekerheid verkregen. Overweeg aanvullende informatie of toetsing bij deze partijen.
Volledige zekerheid: Een assurance- of certificeringsrapport ziet altijd op een afgebakende periode en scope; het dekt nooit alles.	Zie het rapport als momentopname. Gebruik bevindingen als startpunt voor dialoog, risicomanagement en verbetering – niet als eindpunt van toezicht.

Mate van zekerheid

Externe assurance-rapportages verschillen niet alleen in scope, maar ook in de mate van zekerheid:

- ISAE 3402 kent type 1 en type 2:
  - Type 1: de auditor oordeelt of de beschrijving van het systeem van de serviceorganisatie op een bepaalde datum getrouw is, en of de interne beheersingsmaatregelen die bij de doelstellingen horen op die datum adequaat zijn opgezet en geïmplementeerd. De werking over een periode wordt niet getoetst.
  - Type 2: naast bovenstaande oordeelt de auditor óók over de effectieve werking van die maatregelen gedurende een gespecificeerde periode.

    Bestuurders moeten expliciet nagaan welke versie zij ontvangen – een type 1 geeft aanzienlijk minder zekerheid.

- ISAE 3000 en duurzaamheidsassurance:
  In veel duurzaamheidsrapportages wordt nu nog een beperkte mate van zekerheid afgegeven.
  Dat is wezenlijk anders dan de redelijke mate van zekerheid bij veel financiële controles[6].

- ISO-certificering:
  ISO is geen assurance, maar een toets op het aanwezig zijn van een managementsysteem.
  De mate van zekerheid is daarom fundamenteel anders dan bij assurance-opdrachten.

Een rapport kan professioneel en volledig ogen, maar de vorm van toetsing bepaalt hoeveel zekerheid het daadwerkelijk biedt. Bestuurders moeten dit expliciet nagaan.

6 Over assurance bij duurzaamheidsinformatie, zie de brochure: De accountant en het CSRD duurzaamheidsverslag

Signaal 3 |
Nieuwe kaders, nieuwe verantwoordelijkheden

De keten wordt de toetssteen van goed bestuur. Digitalisering, duurzaamheid en geopolitiek versterken elkaar en vergroten de maatschappelijke druk op organisaties om te weten met wie ze samenwerken en wat daar gebeurt. Wie de keten niet kent, verliest regie over risico's én reputatie.

Digitalisering, duurzaamheid, geopolitiek en maatschappelijke verwachtingen ontwikkelen zich niet langer in afzonderlijke domeinen. Ze grijpen in elkaar en versterken elkaars risico's. Organisaties moeten aantonen wat zij zélf doen, maar steeds vaker ook wat hun leveranciers, ketenpartners en onderaannemers doen en hoe die samen bijdragen aan continuïteit, veiligheid en maatschappelijke verantwoordelijkheid.

De nieuwe Europese kaders zoals DORA en NIS2, en de groeiende maatschappelijke druk op duurzaamheid, leggen de lat hoger. Zij vragen om een breed zicht op de keten: niet alleen wie de leveranciers zijn, maar hoe data, processen en verantwoordelijkheden door de keten heen stromen.

Nieuwe Europese kaders voor weerbaarheid

De Europese Unie heeft met DORA (Digital Operational Resilience Act) en NIS2 (Network and Information Security Directive) twee kaders ingevoerd die de digitale weerbaarheid van organisaties versterken.

- DORA richt zich vooral op financiële instellingen en hun kritieke ICT-dienstverleners. Zij moeten aantoonbaar kunnen blijven functioneren bij cyberincidenten en krijgen zwaardere eisen voor risicobeheersing, contractmanagement en teststrategieën.
- NIS2 breidt de zorgplicht voor cyberbeveiliging uit naar vrijwel alle vitale sectoren, waaronder energie, zorg, transport, overheid en digitale infrastructuur, en legt de eindverantwoordelijkheid expliciet bij het bestuur.

Deze Europese kaders zijn geen assurance-standaarden, maar governance-instrumenten die nadruk leggen op ketenverantwoordelijkheid en bestuurlijke eindverantwoordelijkheid. Zij vragen van organisaties dat zij hun uitbestedingsketen volledig in kaart brengen, de kritieke afhankelijkheden begrijpen en actief sturen op continuïteit en herstel.

Beide kaders benadrukken dat weerbaarheid meer is dan techniek: het gaat om governance, samenwerking in de keten en tijdig herstel bij verstoringen.

Voor bestuurders: Controleer of uw organisatie of leveranciers onder DORA of NIS2 vallen, en borg dat verantwoordelijkheden, rapportage en incidentmanagement ook bestuurlijk zijn belegd.

In de praktijk blijkt juist dat zicht vaak beperkt. Als bestuurders onvoldoende overzicht hebben van:

- welke datastromen door de keten gaan,
- op welke plekken data worden verwerkt, opgeslagen of gecombineerd,
- welke beheersingsmaatregelen in de keten ontbreken of afhankelijk zijn van leveranciers,
- en hoe snel incidenten zich kunnen verspreiden binnen de waardeketen,

vergroot dat niet alleen cyber- en operationele risico's, maar ook duurzaamheidsrisico's in brede zin. Van onjuiste rapportages tot het niet naleven van ketenverplichtingen rond milieu, mensenrechten, privacy of DORA/NIS2-eisen. Voor al deze risico's geldt dat verkeerde of incomplete data kunnen leiden tot onjuiste rapportages, onbetrouwbare KPI's en verkeerde besluiten, naast blootstelling aan kwetsbaarheden in de keten.

Zelfs wanneer afzonderlijke processen, digitaal, operationeel, duurzaam of financieel, goed zijn ingericht, ontstaat mogelijke kwetsbaarheid zodra gegevens, systemen of ketenpartners onvoldoende op elkaar aansluiten. Dat maakt deze nieuwe kaders minder een compliance-vraagstuk dan een governance-vraagstuk. Bestuurlijke verantwoordelijkheid staat daarbij centraal. Voor de beheersing van digitale risico's en (IT-) continuïteit ligt deze primair bij bestuur en toezicht (RvB en Rvc/RvT). Europese kaders zoals DORA (artikel 5) en NIS2 (artikel 20) maken expliciet dat organisaties structureel inzicht moeten organiseren in digitale risico's, ketenafhankelijkheden en incidentafhandeling. Uitbesteding ontslaat bestuurders niet van deze verantwoordelijkheid.

BW2:393 lid 4 bepaalt dat de accountant rapporteert over bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking voor zover deze tijdens de controle naar voren komen. Dit schept geen aanvullende controleplicht, maar benadrukt dat signalen over IT-continuïteit wel nadrukkelijk gedeeld moeten worden met bestuur en toezicht wanneer ze worden geconstateerd.

Dit plaatst assurance in perspectief: continuïteit en ketenstabiliteit zijn primair bestuurlijke keuzes; assurance is ondersteunend, nooit vervangend.

Om aan deze verantwoordelijkheid te voldoen, is het noodzakelijk om verschillende disciplines, leveranciers en rapportagelijnen te kunnen verbinden tot één samenhangend risicobeeld, inclusief de dataflow waarop dat beeld gebaseerd is. Een praktische ontwikkelstap is om digitale beheersing niet langer versnipperd te rapporteren via losse compliancerapporten, maar in één integraal kader. De recent gelanceerde International Digital Reporting Standards (IDRS) biedt hiervoor een structuur op basis van COSO en zes materiële onderwerpen, waardoor bestuur en toezicht periodiek een compleet beeld kunnen krijgen van digitale beheersing en IT-continuïteit.

IDRS: integraal rapporteren over digitale beheersing

In 2025 is de finale versie van IDRS gelanceerd (www.ecp.nl/idrs). Deze standaard biedt organisaties één geïntegreerde structuur om intern én/of extern te rapporteren over de brede IT-beheersing. Deze standaard is gebaseerd op COSO en omvat zes materiële onderwerpen:

1. Digital Innovation and Transformation
2. Data & Artificial Intelligence
3. Third Party Management
4. Cybersecurity
5. IT Continuity Management
6. Privacy

Onderliggend aan deze topics liggen veelgebruikte IT-normenkaders. IDRS genereert één integrale rapportage over de beheersing van IT en goed te gebruiken voor bestuurders en leden van de RvC en RvT en kan op termijn andere verplichte rapportages vervangen.

De essentie: digitale weerbaarheid, organisatiecontinuïteit en duurzaamheidsverantwoordelijkheid zijn geen losse thema's meer, maar onderling verbonden ketenelementen.

Welke acties dienen bestuurders hiervoor binnen hun organisatie uit te zetten en zijn voor de commissarissen aandachtspunten van belang om toezicht op te houden:

- Breng dataflows binnen de keten in kaart: waar worden gegevens aangemaakt, verwerkt, verrijkt en doorgegeven?
- Integreer digitale, operationele en duurzaamheidsrisico's in één samenhangend risicobeeld. Daarbij gaat het niet om drie losse compliance-dossiers,

maar om één governancevraagstuk: hoe beïnvloeden deze risico's elkaar, waar versterken ze elkaar en wat betekent dit voor de continuïteit en besluitvorming?

- Zorg dat alle ketendata: financieel, operationeel, IT- en duurzaamheidsgerelateerde, aansluiten op interne controles, IT-systemen, OT-systemen en ketenrapportages.
- Zet internal audit in om de beheersing van de kwaliteit en volledigheid van dataflows, interne controles en ketenrapportages onafhankelijk te toetsen en om te signaleren waar processen of systemen niet op elkaar aansluiten.
- Stel keteneisen die zowel performance, cyberveiligheid als ESG-criteria omvatten.
- Vraag leveranciers om transparantie over datakwaliteit, controles en incidentafhandeling.
- Voorkom 'parallelle werelden': organiseer één geïntegreerde bestuurlijke dialoog over IT-, data-, duurzaamheids- en ketenrisico's. Denk hierbij aan de samenhang tussen financiële verslaggeving, IT-beheersing en (ESG-)keteninformatie.
- Zorg dat zowel RvB als RvC/RvT periodiek integraal inzicht krijgen in IT-beheersing, digitale continuïteit en ketenafhankelijkheden conform de eisen uit DORA en NIS2. Overweeg hiervoor toepassing van IDRS als integraal rapportage-instrument, zodat digitale risico's, thirdparty management en dataflows zichtbaar in één overzicht samenkomen.

Nieuwe kaders vragen niet alleen nieuwe rapportages, maar vooral nieuw leiderschap: weten wat er buiten de poort gebeurt en daar verantwoordelijkheid voor nemen.

Signaal 4 |
Weerbaarheid is een bestuursverantwoordelijkheid

Weerbaarheid is het nieuwe bewijs van beheersing. De vraag is niet óf een verstoring plaatsvindt, maar hoe snel en transparant een organisatie kan herstellen. Bestuurders moeten weerbaarheid actief organiseren, oefenen en rapporteren.

De onzekerheid van de toekomst neemt sneller toe dan organisaties kunnen bijbenen. Cyberaanvallen, verstoringen in logistiek, internationale spanningen of uitval van leveranciers kunnen zich gelijktijdig voordoen en elkaar onverwacht versterken. De vraag is niet óf een verstoring zich voordoet, maar hoe snel de organisatie kan herstellen en wat dat vraagt van de keten waar zij deel van uitmaakt. Weerbaarheid is daarmee geen IT- of crisisthema, maar een expliciete verantwoordelijkheid van zowel bestuur als toezicht: zij moeten borgen dat de organisatie en haar ketenpartners voorbereid zijn op verstoring en herstel.

De NIS2 legt de bestuurlijke eindverantwoordelijkheid voor digitale weerbaarheid expliciet bij het bestuur. Bij nalatigheid kunnen zelfs persoonlijke consequenties volgen. Maar dezelfde logica geldt breder: ook buiten de digitale keten verwachten toezichthouders en stakeholders dat organisaties aantoonbaar inzicht hebben in hun kwetsbaarheden en herstelvermogen.

In de praktijk zien we dat veel organisaties vooral sturen op normale bedrijfsvoering, niet op herstel onder druk. Continuïteitsplannen bestaan vaak, maar zijn generiek, niet getraind of onvoldoende afgestemd met leveranciers. Wanneer één schakel uitvalt, blijkt pas hoe afhankelijk processen, systemen en data van elkaar zijn.

Een goed voorbeeld hiervan is de regionale RIR-oefening (Regionaal Incident Responsteam) in de zorgsector. Tijdens de SRZ-oefening (Samenwerkende Rijnmond Ziekenhuizen[7]) in oktober 2025 moesten bestuurders, CISO's en crisiscoördinatoren aan de hand van een complex scenario en onder tijdsdruk:

- onderscheid maken tussen hoofd- en bijzaken;
- aannames kritisch toetsen aan feiten;
- regionaal opschalen volgens een set afspraken voor regionale opschaling, besluitvorming en samenwerking tijdens crisis, gebaseerd op GRIP[8];
- effectief samenwerken met ketenpartners.

De belangrijkste les uit deze oefening: in een crisissituatie vallen governance en herstelvermogen samen. Niet technologie bepaalt het succes van herstel, maar de mate waarin rollen vooraf zijn belegd, besluitvorming helder is en ketenpartners daadwerkelijk samenwerken.

Weerbaarheid is daarom geen IT-thema, maar een bestuurlijk thema. Het raakt strategie, operatie, financiën én communicatie en bepaalt uiteindelijk de continuïteit van de onderneming. Voor accountants, IT-auditors en internal auditors is dit essentieel: continuïteit is niet

7 Rijnmondse ziekenhuizen versterken samenwerking rondom cybersecurity – Stichting Samenwerkende Rijnmond Ziekenhuizen (stichting-srz.nl) – op basis hiervan heeft de SRZ-oefening plaatsgevonden
8 GRIP staat voor Gecoördineerde Regionale Incidentbestrijdingsprocedure

alleen een financiële of IT-vraag, maar een geïntegreerd governance-vraagstuk waar assurance slechts een deel van afdekt.

Welke acties dienen bestuurders hiervoor binnen hun organisatie uit te zetten en zijn voor de commissarissen aandachtspunten van belang om toezicht op te houden:

- Zet weerbaarheid structureel op de bestuurlijke agenda, als volwaardig onderdeel van strategische besluitvorming en risicodialoog.
- Voer realistische ketenoefeningen uit met bestuur, toezicht, leveranciers en partners gericht op uitval van technologie, data, logistiek of kritieke functies.
- Actualiseer herstel- en continuïteitsplannen op basis van nieuwe risico's, maatschappelijke verwachtingen en Europese regelgeving (zoals DORA, NIS2).
- Laat internal audit niet alleen de continuïteit en weerbaarheid van uw eigen organisatie beoordelen, maar ook die van cruciale ketenpartners: hoe snel kunnen zij herstellen en onder welke voorwaarden?
- Zorg dat besluitvorming onder tijdsdruk rolvast en voorbereid is: escalaties, verantwoordelijkheden en communicatielijnen moeten vooraf helder zijn.
- Rapporteer transparant over herstelvermogen en leerpunten voor organisaties die onder de Corporate Governance Code vallen: expliciteer afhankelijkheden, onzekerheden en herstelstrategie in de VoR.

Signaal 5 |
De auditor als verbinder van vertrouwen

Nederland rekent op zijn auditors: accountants, IT-auditors en internal auditors. Door samenwerking tussen deze disciplines en met toezichthouders wordt ketenweerbaarheid versterkt, en krijgt vertrouwen een bredere basis dan cijfers alleen.

Bestuurders moeten kunnen vertrouwen op informatie die klopt, op risico's die in beeld zijn en op een governanceketen die doet wat zij belooft. In een wereld waarin processen, data en ketenpartners steeds sterker met elkaar verweven zijn, vraagt dat om samenwerking tussen assurance-disciplines en om helderheid over wie waarvoor staat.

De accountant en IT-auditor vervullen daarin een unieke rol. Zij combineren onafhankelijkheid met vaktechnische en inhoudelijke deskundigheid, zien organisaties van binnen én van buiten, en kunnen ketenrisico's duiden op een manier die bestuurders helpt juiste keuzes te maken.

Maar zij doen dat niet alleen. Internal audit – als derde lijn binnen veel organisaties – heeft vaak als eerste zicht op procesrisico's, operationele afhankelijkheden en knelpunten in de keten. Wanneer internal audit signalen tijdig deelt en de accountant en IT-auditor deze duiden in samenhang met externe assurance, ontstaat een veel rijker beeld van de werkelijkheid. Iedere functie kijkt vanuit een andere invalskoek – en juist dat maakt ze aanvullend:

- internal audit toetst de governance en beheersing, geeft intern zekerheid, uitgaande van de strategische doelen en risico's van de organisatie;
- de accountant en IT-auditor geven onafhankelijk assurance aan externe belanghebbenden en verbinden de inzichten met governance en verslaggeving.

Ook toezichthouders zoals DNB en AFM leveren een belangrijke bijdrage. In hun analyses en good practices over outsourcing, ketenrisico's en digitale afhankelijkheid benadrukken zij dat organisaties niet alleen hun eigen beheersing op orde moeten hebben, maar ook actief moeten sturen op de keten waar zij van afhankelijk zijn.

De echte meerwaarde ontstaat wanneer deze perspectieven samenkomen: bij bestuur, bij toezicht én bij het auditberoep in brede zin.

Welke acties dienen bestuurders hiervoor binnen hun organisatie uit te zetten en zijn voor de commissarissen belangrijke aandachtspunten om toezicht op te houden:

- Zie de accountant, IT-auditor en internal auditor als sparringpartner in de dialoog over ketenrisico's en continuïteit.
- Stimuleer samenwerking tussen internal audit, de accountant en de IT-auditor zodat bestuurders één samenhangend en integraal beeld krijgen van risico's.
- Zet internal audit expliciet in om strategische en operationele (keten)risico's onafhankelijk te toetsen, zodat kwetsbaarheden tijdig in beeld komen

en de dialoog met externe assurance goed is onderbouwd.
- Gebruik good practices van toezichthouders (zoals AFM en DNB) om governance, risicobeheersing en rapportage te versterken.
- Vraag niet om méér zekerheid, maar om betere duiding van wat zekerheid wel en niet betekent in een verweven keten.

Zoals al vaker is benadrukt: de accountant is niet de vertrouwenspersoon van één onderneming, maar van het maatschappelijk verkeer dat op die onderneming vertrouwt. Dat betekent dat bestuurders mogen rekenen op helderheid over wat assurance wél en niet dekt, op tijdige signalen wanneer informatie ontbreekt of ketenrisico's buiten beeld vallen en op een scherpe duiding van aannames waarop hun besluitvorming rust.

Maar het betekent ook dat accountants, IT-auditors en internal auditors grenzen moeten aangeven: waar de door hen geboden zekerheid ophoudt, waar afhankelijkheden niet toetsbaar zijn, en waar aanvullende maatregelen buiten de scope van assurance liggen. Juist dat helpt bestuurders om hun eigen verantwoordelijkheid goed te kunnen nemen.

In een wereld waarin organisaties steeds meer leunen op ketens, is deze wederkerigheid essentieel: bestuurders die het juiste gesprek voeren over afhankelijkheden en onzekerheden, én auditors die helpen dat gesprek scherp, feitelijk en volledig te maken.

Wat bestuurders wél en níet mogen verwachten van accountants, IT-auditors en internal auditors als het gaat om externe respectievelijk interne zekerheid

Wat bestuurders wél mogen verwachten:
- Duidelijkheid over wat assurance wél en niet dekt – inclusief scope, aannames, carve-outs en beperkingen.
- Uitleg en duiding van ketenrisico's en data-flows voor zover deze relevant zijn voor de opdracht.
- Samenhang tussen financiële, digitale, operationele en duurzaamheidsinformatie: geen eilandjes maar één verhaal.
- Signalering van blinde vlekken: wanneer cruciale afhankelijkheden, data of processen buiten beeld dreigen te raken.

Wat bestuurders níet mogen verwachten:
- Volledige zekerheid over de keten: geen enkele assurancevorm kan alle schakels, onderaannemers en risico's afdekken.
- Dat alle risico's zijn afgedekt: assurance is altijd beperkt tot een afgebakende scope en periode.
- Een uitgebreide adviesrol van de accountant: wet- en regelgeving begrenzen bewust de omvang van de (natuurlijke) adviesfunctie.

Conclusie:
Bestuurders mogen helderheid en samenhang verwachten, maar geen absolute zekerheid. En auditors moeten transparant zijn over de grenzen van hun oordeel – om ruimte te maken voor het juiste gesprek.

Signaal 6 |
Auditdisciplines in beweging: samenwerken aan ketenzekerheid

De complexiteit van digitale en operationele ketens groeit sneller dan de huidige assurance-instrumenten. Alleen wanneer accountants, IT-auditors en internal auditors elkaar versterken, ontstaat voor bestuurders een risicobeeld dat de werkelijkheid recht doet.

De werkelijkheid ontwikkelt zich sneller dan de auditdisciplines kunnen bijbenen. De wereld waarover accountants, IT-auditors en internal auditors zekerheid geven, verandert sneller dan de instrumenten waarmee die zekerheid traditioneel wordt verstrekt. Digitalisering, AI, cloud-afhankelijkheid, internationale dataflows en ketenuitbesteding zorgen ervoor dat geen enkele discipline nog alleen een volledig risicobeeld kan overzien. Het beroep moet daarom zélf in beweging komen.

De accountant en de IT-auditor zijn uit elkaar gegroeid, terwijl de praktijk juist om integratie vraagt.

In de afgelopen twintig jaar zijn financiële assurance (RA) en IT-assurance (RE) steeds verder van elkaar losgekomen. Wetgeving zoals de Wet toezicht accountantsorganisaties (Wta), specialisatie van het vak en gescheiden opleidingspaden hebben die afstand vergroot. Maar de werkelijkheid van vandaag vraagt het omgekeerde:

- IT is de ruggengraat van vrijwel elk proces: financieel, operationeel, logistiek, zorg, productie én duurzaamheid.
- Ketenrisico's ontstaan steeds vaker in systemen, data, interfaces en bij onderaannemers; daar waar IT-auditors dagelijks werken.
- Bestuurders en toezichthouders zijn wettelijk verantwoordelijk voor de continuïteit en IT-beheersing van hun organisatie, daarom verwachten zij dat accountants hierover zekerheid kunnen geven. In de praktijk kan de accountant binnen de jaarrekeningcontrole echter alleen zekerheid geven over díe IT-processen die relevant zijn voor de financiële verslaggeving, niet over de volledige digitale keten of IT-continuïteit.

Daarom is helderheid nodig: over cloudketens, onderaannemers en digitale continuïteit kan géén enkele partij volledige zekerheid geven. Wat accountants en IT-auditors wél kunnen, is inzichtelijk maken wáár de grenzen van zekerheid liggen en welke risico's daarmee onvermijdelijk bij bestuurders zelf blijven.

Door regelgeving van accountants (Standaard 610)[9] wordt internal audit in de praktijk nog te weinig benut als structurele schakel tussen organisatie en externe assurance. Terwijl juist internal audit vaak als eerste zicht heeft op procesrisico's, operationele afhankelijkheden, datastromen en knelpunten in de keten, omdat de functie continu in contact staat met de business. Daardoor kan internal audit tijdig signaleren waar aannames niet kloppen, waar beheersing afneemt en waar afhankelijkhe den groter worden dan bestuurders denken.

9 Zie voor nadere toelichting op de toepassing van COS 610 de Nadere Voorschriften Controle- en Overige Standaarden (NV COS), die de rol van internal audit binnen de bredere assurance- en controlematrix verduidelijken.

Het gevolg: een kloof tussen wat bestuurders dénken dat de accountant doet en wat accountants en IT-auditors binnen wet- en regelgeving daadwerkelijk kúnnen doen. Die kloof moet worden gedicht, niet door grenzen op te rekken, maar door beter samen te werken.

Om bestuurders een completer en betekenisvoller risicobeeld te geven, zullen de accountant, de IT-auditor en internal audit elkaar veel vaker moeten opzoeken. Niet door rollen te vermengen, maar door:

- *Gezamenlijke risicoduiding*
  Welke afhankelijkheden zijn materieel? Welke data zijn kritisch? Waar in de keten ontstaan risico's die nu buiten beeld vallen?

- *Gedeeld inzicht in dataflows, IT-architectuur en procesketens*
  Waar ontstaan risico's met financiële impact die technisch beginnen – of juist andersom?

- *Afstemming in werkzaamheden*
  Zodat bevindingen uit IT-audits en internal audit daadwerkelijk landen in de financiële oordeelsvorming, en niet als parallel spoor blijven liggen.

- *Een gedeelde taal naar bestuurders*
  Die duidelijk maakt wat assurance wél dekt, wat níet, en welke aanvullende beheersing een organisatie zélf moet inrichten.

- *Gezamenlijk spiegelen op de risico's die het bestuur moet verantwoorden*
  Zodat strategische afhankelijkheden, datastromen, IT-risico's en ketenkwetsbaarheden compleet en consistent worden besproken, vóórdat zij in het bestuursverslag landen.

Daarnaast geldt dat IT-auditors in de praktijk vaak vooral gericht zijn op de CIO-kolom en de technische omgeving en minder gericht op hoe ICT past in het behalen van de bedrijfsdoelstellingen. Daardoor sluiten hun bevindingen niet altijd vanzelf aan op governance, strategie en besluitvorming. Precies daar ligt een belangrijke ontwikkelkans: wanneer IT-auditors nadrukkelijker kijken naar bestuurlijke materialiteit - welke risico's er écht toe doen voor bestuur en toezicht - groeit hun toegevoegde waarde aanzienlijk. Dat vraagt om een verbreding van perspectief, zodat technische bevindingen niet op zichzelf staan maar worden verbonden met strategische afhankelijkheden, ketenrisico's en continuïteitsvraagstukken.

Ook de accountant heeft een expliciete ontwikkelopgave. Van accountants wordt steeds meer verwacht dat zij niet alleen financiële processen begrijpen, maar ook de digitale en ketenafhankelijkheden die deze processen dragen. Dat betekent: voldoende digitale geletterdheid, het vermogen om IT-auditbevindingen bestuurlijk te duiden en de bereidheid om internal audit actief te betrekken. Niet om zelf IT-specialist te worden, maar om te zien waar financiële materialiteit ontstaat in digitale ketens en bestuurders daarin helder, feitelijk en zonder overschatting van zekerheid te begeleiden.

De auditdisciplines moeten zich opnieuw met elkaar verbinden. IT is inmiddels de kern van vrijwel ieder bedrijfsproces. Daarmee is IT-assurance geen aanvullende specialisatie meer, maar een voorwaarde voor moderne governance. Financiële en IT-assurance kunnen niet langer naast elkaar bestaan als parallelle werelden: zij moeten elkaar versterken, zowel in planning, risicoduiding als in communicatie richting bestuurders.

Internal audit heeft zicht op processen en risico's door de hele organisatie. Daardoor ziet zij vaak eerder dan anderen waar afhankelijkheden ontstaan, waar controles ontbreken of waar knelpunten in de keten zichtbaar worden. Die inzichten zijn waardevol voor zowel accountant als IT-auditor, omdat zij helpen om financiële en digitale risico's in samenhang te beoordelen.

Het beroep moet daarom reflecteren of het huidige assurance-instrumentarium nog past bij de moderne ketenrealiteit: AI-risico's, cloud-afhankelijkheid, data-intensieve processen en steeds langere, complexere dienstverleningsketens. Nieuwe vormen van assurance ontwikkelen kost tijd, maar een sterkere en meer geïntegreerde samenwerking kan vandaag al beginnen.

In dat licht wordt ook gewerkt aan versterking van de digitale component in de controlepraktijk. De aandacht voor IT-continuïteit binnen de jaarrekeningcontrole neemt toe. NBA en NOREA ontwikkelen gezamenlijk een handreiking om accountants te ondersteunen bij het beoordelen en duiden van IT-continuïteitsrisico's en de mogelijke impact daarvan op de continuïteit van de organisatie (op basis van BW2:393 lid 4). Deze handreiking wordt in de loop van 2026 verwacht en bouwt voort op bestaande verplichtingen.

Welke acties dienen accountants, IT-auditors en internal auditors te nemen zodat Nederland kan blijven rekenen op zijn accountants en IT-auditors:

- Werk vanuit één gedeeld risicobeeld bij keten-, IT- en dataflowrisico's, zodat financiële, operationele en technologische afhankelijkheden zichtbaar samenkomen.
- Bouw aan integrale assurance, waarin financiële, operationele en IT-werkzaamheden logisch op elkaar aansluiten en bevindingen niet als parallelle sporen blijven liggen.
- Benut internal audit als structurele schakel tussen operatie, risico, IT-ketens en rapportage, juist omdat internal audit doorlopend zicht heeft op de afhankelijkheden en beheersing.
- Versterk wederzijds begrip: accountants meer aandacht voor digitale afhankelijkheden; IT-auditors meer aandacht voor governance (bestuurlijke duiding), strategie en materialiteitsbesef.
- Communiceer expliciet richting bestuurders en toezichthouders wat de accountant, de IT-auditor en internal audit wél en níet in scope nemen. Lever bestuur en toezicht (RvC/RvT) periodiek een samenhangend inzicht in IT-beheersing, digitale continuïteit en ketenafhankelijkheden op basis van bevindingen uit reguliere controle- en auditwerkzaamheden. Dit helpt bestuurders hun wettelijke verantwoordelijkheid onder BW2[10], DORA en NIS2 waar te maken en voorkomt parallelle risicobeelden.
- Reflecteer als beroepsgroepen op de toekomstbestendigheid van bestaande assurance-instrumenten zoals ISAE 3000, ISAE 3402 en ISO-certificeringen, gezien de snelheid van digitale en geopolitieke ontwikkelingen.
- Wees zichtbaarder als duider van onzekerheden, zonder in een adviesrol te vervallen, door feiten, aannames en grenzen helder te maken voor bestuur en toezicht.

De samenleving rekent op betrouwbare en transparante informatie én op auditdisciplines die meegroeien met de realiteit van vandaag. Het bestuur blijft verantwoordelijk voor de keuzes, afhankelijkheden en risico's in de keten. Maar accountants, IT-auditors en internal audit dragen bij door die verantwoordelijkheid beter te onderbouwen, te spiegelen en te versterken. Ketenzekerheid is geen solotaak: het is een gezamenlijke opdracht waarin de auditdisciplines een belangrijke voorstrekkersrol hebben.

10 BW2:393 lid 4 verplicht de accountant alleen te rapporteren over bevindingen rond betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking voor zover deze tijdens de jaarrekeningcontrole worden geconstateerd. Deze oproep ziet op het doelmatig delen van relevante inzichten, niet op verruiming van de wettelijke onderzoeksplicht.

Wat morgen doen: werk aan de bestuurlijke cyclus van ketenvertrouwen

Ketenweerbaarheid vraagt om structurele aandacht, niet om een eenmalige analyse. Deze cyclus helpt bestuurders en commissarissen om grip te houden op afhankelijkheden die direct raken aan continuïteit, digitale veiligheid, logistiek, data-integriteit en maatschappelijke verantwoordelijkheid.

1. Breng uw keten in kaart, inclusief schaduwkanten

Zorg voor een actueel en compleet overzicht van:

- kritieke leveranciers, platforms en datadienstverleners;
- onderaannemers en grensoverschrijdende schakels;
- dataflows: waar data worden aangemaakt, verwerkt, opgeslagen en doorgegeven;
- leveranciers of platformen waarop u structureel bent geconcentreerd.

Waarom: u kunt pas sturen op risico's die u kent. Bij veel organisaties blijkt dat overzicht beperkt of versnipperd aanwezig.

2. Voer een ketenbrede risicoanalyse uit – één integraal risicobeeld

Digitalisering, operatie, financiën, logistiek, compliance en ESG hangen samen. Breng risico's daarom gezamenlijk in kaart:

- digitale risico's (cyber, cloud, interfaces, onderaannemers);
- operationele en logistieke afhankelijkheden;
- financiële kwetsbaarheden;
- ESG- en datakwaliteitsrisico's;
- geopolitieke en leveringsrisico's.

Actualiseer dit beeld minimaal jaarlijks, of sneller bij technologische of geopolitieke veranderingen.

3. Maak betere afspraken – contracten die werken in de wereld van nu

Actualiseer contracten en zorg dat ze aansluiten bij moderne risico's en nieuwe wetgeving:

- continuïteitsafspraken, fallbackopties en exitstrategieën;
- right-to-audit en rapportageverplichtingen (incl. incidentmeldingen);
- afspraken over wijziging van eigendom of zeggenschap (change of ownership), inclusief meldplicht en herbeoordeling van continuïteits- en risicoprofiel;
- keten-eisen voor cybersecurity, AI-gebruik en databeveiliging;
- verplicht inzicht in onderaannemers en doorleveranciers;
- afspraken over datakwaliteit, ESG-informatie en data-integriteit.

Verouderde contracten zijn één van de grootste blinde vlekken in ketenrisico's.

4. Richt structureel ketenoverleg en monitoring in

Plan periodiek overleg met ketenpartners en leveranciers over:

- prestaties, incidenten, near-misses;
- risico's, trends en keteneffecten;
- wijzigingen in processen, systemen of datastromen;
- afhankelijkheden van onderaannemers.

Zorg voor indicatoren voor digitale, operationele en maatschappelijke risico's en maak dit een vast agendapunt in de governance.

5. Beoordeel assurance kritisch en weet wat het níet zegt

ISAE-rapportages, SOC 2 en ISO-certificaten zijn waardevol, maar geven geen volledige zekerheid.

- Begrijp de scope: wat wordt wel en niet onderzocht?
- Let op carve-outs: welke onderdelen blijven buiten beeld?
- Check user controls: welke beheersmaatregelen moet u zelf uitvoeren?
- Gebruik auditors als duiders, niet als vervangers van uw oordeel.
- Kijk of assurance past bij uw ketenrisico's – en voeg waar nodig aanvullende beheersing toe.

Assurance is een puzzelstuk. De keten blijft uw eigen verantwoordelijkheid.

6. Test herstelvermogen; resillence is de nieuwe toetssteen van governance

Organiseer realistische oefeningen waarin uitval van leveranciers, platforms of datadiensten wordt nagebootst.

- betrek bestuurders, commissarissen, internal audit en leveranciers;
- oefen besluitvorming onder tijdsdruk;
- test communicatie, escalatie en herstel;
- gebruik praktijkvoorbeelden zoals sectorbrede oefeningen en regionale RIR-initiatieven.

In crisissituaties vallen governance en veerkracht samen.

7. Leer en verbeter continu; weerbaarheid groeit door iteratie

Gebruik incidenten, audits, near-misses en ketengesprekken om:

- afspraken te actualiseren;
- dataflows te verbeteren;
- concentratierisico's te verminderen;
- governance te versterken;
- samenwerking met accountants, IT-auditors en internal audit te verdiepen.

Weerbaarheid ontstaat niet door regels, maar door herhaling en verbetering.

8. Onderzoek alternatieven; afhankelijkheid vraagt strategie

Veel sectoren steunen op enkele dominante leveranciers. Zelfs met perfecte assurance blijft dat een strategisch risico.

- onderzoek alternatieve leveranciers en interoperabiliteit;
- beoordeel of afhankelijkheid past bij uw risicobereidheid;
- maak exit-opties onderdeel van governance;
- bespreek dit regelmatig op bestuurs- en RvC-niveau.

Assurance vermindert risico's, maar heft afhankelijkheid nooit op

Ketenvertrouwen bouwt u niet in één keer. Het begint bij inzicht. Het groeit door samenwerking. En het wordt versterkt door transparantie, realistische testen en governance die werkt wanneer het echt spannend wordt. Wie vandaag start met deze cyclus, versterkt morgen al de continuïteit én maatschappelijke betrouwbaarheid van zijn organisatie.

Tot slot:
Vertrouwen vraagt om actie

De risico's in ketens worden groter, complexer en minder voorspelbaar. Digitalisering, geopolitiek, data-afhankelijkheden en maatschappelijke verwachtingen versterken elkaar en geen enkele organisatie kan die dynamiek alleen beheersen.

Wat deze Publieke managementletter laat zien, is dat vertrouwen in de keten niet ontstaat door méér rapporten, maar door scherp inzicht en transparante risicorapportages door het bestuur aangevuld met beter samenspel tussen bestuurders, toezichthouders, accountants, IT-auditors en internal audit. Vertrouwen vraagt dat het bestuur expliciet maakt welke afhankelijkheden en onzekerheden er zijn, en dat de auditdisciplines helpen om die inzichten te duiden en te versterken.

Ketenweerbaarheid ontstaat wanneer bestuurders hun afhankelijkheden expliciet maken, leveranciers aanspreken op transparantie en alternatieven verkennen; wanneer accountants, IT-auditors en internal auditors duidelijk aangeven wat externe en interne assurance wél en niet dekt; en wanneer de auditdisciplines zelf de handen ineenslaan om de praktijk bij te houden die sneller verandert dan de instrumenten waarmee we haar beoordelen.

De samenleving rekent op betrouwbare informatie en op organisaties die voorbereid zijn op verstoring. Die betrouwbaarheid begint bij bestuurders die eerlijk zijn over onzekerheden en afhankelijkheden, verlangt samenwerking tussen disciplines en ketenpartners, en wordt verankerd door bestuurlijke keuzes die verder kijken dan de eigen organisatiegrenzen. Zo ontstaat niet alleen beter inzicht, maar ook het herstelvermogen dat nodig is in een wereld waarin verstoringen elkaar steeds sneller opvolgen.

De realiteit dringt zich op. En wie vandaag begint met inzicht, dialoog en samenwerking, bouwt morgen aan een sterkere organisatie én een veerkrachtigere keten.

Ketenvertrouwen ontstaat niet vanzelf; het vraagt inzicht, samenwerking en het lef om onzekerheden bespreekbaar te maken.

Afkortingen

AFM	Autoriteit Financiële Markten
COSO	Committee of Sponsoring Organizations of the Treadway Commission (raamwerk voor interne beheersing en risicomanagement)
CSRD	Corporate Sustainability Reporting Directive
DNB	De Nederlandsche Bank
DORA	Digital Operational Resilience Act
ESG	Environmental, Social & Governance
IDRS	International Digital Reporting Standards
IIA	Instituut van Internal Auditors (Nederland)
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
NBA	Koninklijke Nederlandse Beroepsorganisatie van Accountants
NIS2	Network and Information Security Directive (EU)
NOREA	Nederlandse Orde van Register EDP-auditors (IT-auditors)
NV COS	Nadere voorschriften controle- en overige standaarden
PML	Publieke Managementletter
RA	Registeraccountant
RE	Register EDP-auditor (IT-auditor)
RvA	Raad voor Accreditatie
RvB	Raad van Bestuur
RvC	Raad van Commissarissen
RvT	Raad van Toezicht
SOC	Service Organization Control-rapport
VoR	Verklaring omtrent Risicobeheersing
Wta	Wet toezicht accountantsorganisaties

Colofon

Kennis delen

In het NBA beleidsprogramma Kennis Delen wordt de kennis van accountants collectief ingezet om vroegtijdig risico's te detecteren in maatschappelijke sectoren of relevante thema's. Het accent ligt hierbij op risico's op het gebied van bestuur, bedrijfsvoering, verslaggeving en controle.

Deze gezamenlijke publicatie van de NBA Signaleringsraad, NOREA en IIA Nederland heeft als doel om bestuurders en toezichthouders te informeren over de toenemende kwetsbaarheid van ketens, en om helderheid te bieden over de rol van accountants, IT-auditors en internal audit bij het duiden van ketenrisico's, afhankelijkheden en zekerheid.

Signaleringsraad
prof. dr. Leen Paape RA RO CIA (vz)
drs. Anoek Bastiaens RA
Arnout van Kempen CISA

NOREA
drs. Marc Welters RE RA CRISC

IIA Nederland
drs. Frans Eusman

Programmateam Kennis Delen
Jan Jaap Boontjes MA
drs. Robert Mul MPA

Penvoerder
drs. Erik Hessels RA CRMA
Beleidsadviseur Internal Audit & Governance

Met dank aan:
NOREA en IIA Nederland voor inhoudelijke bijdrage, reflectie en co-creatie

Meer informatie

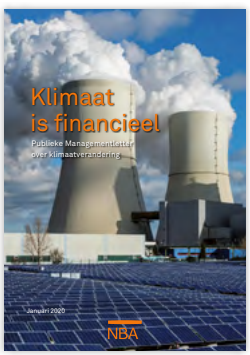
Een publieke managementletter is één van de publicatievormen van het beleidsprogramma Kennis Delen. Daarnaast verschijnen ook open brieven of discussierapporten.

Inmiddels heeft de NBA-Signaleringsraad de volgende publicaties uitgebracht:

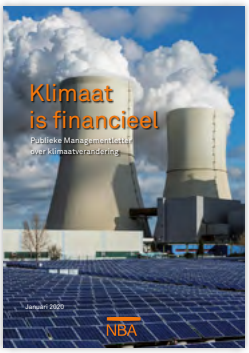
- 2024: De verandering naar een nieuw pensioen
- 2023: Zicht op omschakeling
- 2022: Scherp op fraude
- 2021: Corona
- 2020: Klimaat is financieel
- 2019: Betaald voetbal / Notariaat
- 2018: Commercieel Vastgoed / Trustkantoren
- 2017: Woningcorporaties
- 2016: Cybersecurity / Energiesector / Wetgevingslasten
- 2015: Curatieve zorg / Horeca
- 2014: Life sciences / Banken
- 2013: MBO-scholen / Risicomanagement / Transport en Logistiek
- 2012: Gemeenten / Toon aan de Top / Goede Doelen
- 2011: Commercieel Vastgoed/ Pensioenen / Glastuinbouw
- 2010: Verzekeringen / Langdurige Zorg

Alle publicaties zijn openbaar en bedoeld voor een breed publiek

Publieke Managementletters (PMLs) uitgebracht in 2010-2025



Publieke Managementletters (PMLs) uitgebracht in 2010-2025



Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Mercuriusplein 3
2132 HA Hoofddorp
Postbus 242
2130 AE Hoofddorp

T 088 4960 301
E nba@nba.nl
I www.nba.nl

2026001