



Waarde toevoegen in tijden van verandering

Een digitaal kompas voor auditcommissies



Herziene uitgave
Juni 2025

www.pwc.nl/corporate-governance



Waarde toevoegen in tijden van verandering

Een digitaal kompas voor auditcommissies

Nieuw in deze versie
d.d. juni 2025

Beste commissaris/toezichthouder, beste lezer,

Met trots delen we de nieuwste versie van onze publicatie “Waarde toevoegen in tijden van verandering”. Sinds de lancering in 2019 richten we ons op het voortdurend aanpassen en actualiseren van inzichten die relevant zijn voor leden en voorzitters van auditcommissies. Ons doel is om een digitaal kompas te bieden dat richting geeft in de dynamische wereld waarin we opereren. Door samen te werken, leren en innoveren, hopen we een positieve impact te maken in tijden van verandering.

In deze herziene uitgave van juni 2025 hebben we belangrijke veranderingen en updates aangebracht ten opzichte van de versie van 2021. We hebben onder meer een verdieping aangebracht in de Corporate Impact, Control & Compliance en Corporate Reporting hoofdstukken met de meest recente wetgeving en praktijkvoorbeelden. Daarnaast is aandacht besteed aan nieuwe maatschappelijke discussies en regelgeving zoals de Corporate Sustainability Reporting Directive en de wijzigingen in de accountancysector. Deze elementen onderstrepen ons streven om proactief in te spelen op de veranderende behoeften van de sector en de maatschappij.

Tot slot willen we de kracht van samenwerking benadrukken. Diversiteit en perspectieven samenbrengen blijft een sleutel tot innovatie en effectiviteit. We nodigen u daarom van harte uit om met ons in gesprek te blijven en uw ervaringen, inzichten en suggesties te delen. U kunt contact met ons opnemen via nl_commissarissenontmoetingen@pwc.com

Ik wens u veel leesplezier!

Jacobina Brinkman

Managing partner Commissarissenontmoetingen

Waarde toevoegen in tijden van verandering

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie



De omgeving waarin organisaties opereren verandert voortdurend en ingrijpend. Nieuwe toezichtthema's zoals duurzaamheid, AI, digitalisering, cybersecurity en turbulente geopolitieke ontwikkelingen hebben hun weg gevonden naar de agenda. Governance is eveneens in beweging: de focus is verschoven van winstmaximalisatie en aandeelhouderswaarde op korte termijn naar duurzame langetermijnwaardecreatie voor een brede groep stakeholders. Dit digitaal kompas wil niet alleen de basisbeginselen voor een goed functionerende auditcommissie aanreiken, maar ook richting geven in deze continue veranderende omgeving door het bieden van inzichten en best practices.

Duurzaamheid en lange termijn waardecreatie

In dit kader zijn duurzaamheid en langetermijnwaardecreatie thema's die organisaties vandaag de dag niet meer kunnen negeren. Medewerkers, klanten, leveranciers en de samenleving verwachten dat organisaties zich bewust zijn van hun maatschappelijke impact en verantwoordelijkheid nemen. Duurzaamheid kan ook een strategisch voordeel bieden ten opzichte van de concurrentie. Het begrip 'duurzaam' betekent niet alleen bijdragen aan het behoud van onze planeet, maar ook het waarborgen van de langetermijnwaardecreatie en het voortbestaan van de organisatie voor alle belanghebbenden.

De rol van de Corporate Governance Code

De Nederlandse Corporate Governance Code benadrukt het belang van langetermijnwaardecreatie, het zorgvuldig afwegen van belangen van stakeholders en het oog hebben voor de bredere context waarin de organisatie opereert. Duurzaam handelen gaat niet alleen over de continuïteit van de organisatie, maar biedt ook een tegenwicht tegen de jarenlange focus op aandeelhouderswaarde en het behalen van financiële doelen op korte termijn. De auditcommissie en de rest van de raad van commissarissen spelen een cruciale rol in deze omslag.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Interne beheersing en risicobeheer

De aandacht voor interne beheersing is de afgelopen jaren toegenomen. De auditcommissie speelt hierin een cruciale rol. Zij ziet toe op de effectiviteit van de interne beheersingssystemen en risicobeheersing binnen de organisatie. Dit omvat het beoordelen van de interne controles, het evalueren van de risico's en het waarborgen dat er adequate maatregelen zijn genomen door het management om deze risico's te beheersen. De recent ingevoerde verklaring omtrent risicobeheersing in de Corporate Governance Code benadrukt het belang van een gedegen interne controle en risicobeheer. Hoewel raden van commissarissen en organisaties hier nog mee moeten leren werken, biedt het een kader voor verdere verbetering.

Digitale transformatie en cybersecurity

Daarnaast is het digitale tijdperk angebroken, wat zowel risico's als kansen met zich meebrengt. Cybersecurity en fraud risk assessment zijn cruciale aandachtspunten geworden, aangezien organisaties die lichtzinnig omgaan met de bescherming van hun IT-systemen en gegevensbestanden enorme risico's lopen. Privacywetgeving is aangescherpt, wat een uitdaging kan vormen bij de inzet van data in bedrijfsprocessen, maar ook compliance- en reputatierisico's met zich meebrengt.

Geopolitieke ontwikkelingen en veerkracht

Turbulente geopolitieke ontwikkelingen hebben eveneens invloed op de bedrijfsvoering en vereisen dat organisaties flexibel en veerkrachtig zijn. De verklaring omtrent risicobeheersing in de Corporate Governance Code benadrukt het belang van een gedegen interne controle en risicobeheer om deze uitdagingen het hoofd te bieden.

Tot slot

Deze publicatie fungeert als een digitaal kompas dat voorzitters en leden van auditcommissies richting geeft om waarde toe te voegen in tijden van verandering. We nodigen u graag uit met ons op reis te gaan: hebt u best practices, mist u onderwerpen, zoekt u naar verdieping? Deel het met ons, zodat we dit digitale kompas steeds opnieuw kunnen ijken aan de voortdurend veranderende behoefte aan kennis en inzichten van auditcommissieleden in de praktijk.

Jacobina Brinkman



Navigatiescherm

Met één klik naar relevante toezichtthema's voor de auditcommissie



6

1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen



32

2. Continuïteit - Duurzame langetermijnwaardecreatie

1. Toetsen strategische besluitvorming
2. Beoordelen strategie, business- en investeringsplannen
3. Monitoren van het waardecreatieproces
4. Signaleren van risico's



40

3. Corporate impact - maatschappelijke waardecreatie

1. Corporate impact integreren in de strategie
2. Corporate impact integreren in de bedrijfsvoering
3. Corporate impact integreren in de verslaglegging



52

4. Control & Compliance

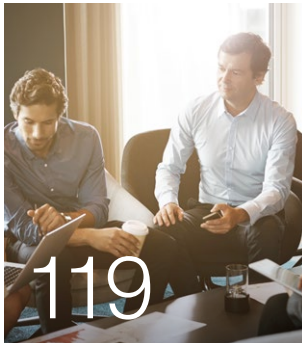
1. Beoordelen van de risico's
 2. Monitoren van de interne risicobeheersings- en controlesystemen
 3. Afstemmen met Internal Audit
 4. Afstemmen met de externe accountant
 5. Interne en externe verantwoording
 6. Enkele risicocategorieën uitgelicht
- Bijlagen



104

5. Cultuur en gedrag

1. Toezicht op de *purpose* en de kernwaarden
2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
3. Meten en monitoren van cultuur en gedrag
4. Toetsen van de gedragscode
5. Voorkomen misstanden en onregelmatigheden
6. Verantwoording afleggen over cultuur en gedrag



119

6. Checks & Balances

- A. De relatie met Internal Audit
 - B. De relatie met de externe accountant
- Bijlagen



150

7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving
 2. Beoordelen van het bestuursverslag
 3. Beoordelen van de financiële informatie buiten de jaarrekening
- Bijlagen



174

8. Misstanden en onregelmatigheden – wat te doen?

1. Meldingen van misstanden en onregelmatigheden
2. Wanneer een onderzoek en door wie?
3. Het samenstellen van het onderzoeksteam
4. Bepalen scope en procedures onderzoek
5. De uitvoering van het onderzoek
6. Communiceren over de voortgang van het onderzoek
7. Het herstelplan
8. Na de crisis: trek de lessen



188

9. Communicatie

1. Communiceren met het bestuur
 2. Communiceren met de raad van commissarissen
 3. Communiceren met stakeholders
- Bijlagen



Commissie

Samenstelling, werkwijze en evaluatie

01

1. Commissie - samenstelling, werkwijze en evaluatie

- 1. Commissie
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
 - 4. Vergaderingen
 - 5. Evaluatie van de auditcommissie
 - Bijlagen
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De meerwaarde van de auditcommissie wordt bepaald door de robuustheid van de basis: heldere afspraken over rol en verantwoordelijkheden, een diverse en onafhankelijke samenstelling met de juiste expertise, een efficiënte vergaderroutine en een effectieve voorzitter.

Wanneer een auditcommissie instellen?

Organisaties van openbaar belang (OOB's), zoals beursgenoteerde ondernemingen, banken en verzekeringsmaatschappijen, moeten in principe verplicht een auditcommissie instellen, volgens het Besluit instelling auditcommissie (hierna: Besluit-AC).

Er kan ook een ander orgaan worden aangewezen dat de taken van de auditcommissie uitoefent. Het ligt voor de hand dat die taken in dat geval worden vervuld door de raad van commissarissen of bij een one-tier board door de niet-uitvoerende leden van het bestuur. In deze gevallen gelden dezelfde eisen die aan de deskundigheid en onafhankelijkheid van de leden van de auditcommissie worden gesteld. In het jaarverslag moet aangegeven worden bij welk ander orgaan de taken van de auditcommissie zijn belegd en moet de samenstelling daarvan worden vermeld.

Er zijn vier vrijstellingen mogelijk van de verplichte instelling tot een auditcommissie of een vergelijkbaar orgaan (zie daarvoor bijlage IA). Een in Nederland regelmatig toegepaste vrijstelling heeft betrekking op dochtermaatschappijen, waarvan de moederorganisatie ook een auditcommissie heeft, die aan de Europese vereisten voldoet.

De verplichting tot het instellen van een auditcommissie geldt ook voor de organisaties die vanaf 1 januari 2020 zijn aangemerkt als OOB: netbeheerders, grote pensioenfondsen, grote instellingen voor het wetenschapsbeleid (KNAW, KB en NWO) en woningcorporaties met meer dan vijfduizend verhuureenheden.

De Nederlandse Corporate Governance Code 2022 (verder: de Code) geeft het volgende aan over de instelling van een auditcommissie: als de raad van commissarissen uit meer dan vier personen bestaat, dan stelt deze uit zijn midden een auditcommissie in (naast een remuneratiecommissie en een selectie- en benoemingscommissie).



In dit hoofdstuk komen de volgende onderwerpen aan de orde:

- 1. Het reglement
- 2. De samenstelling
- 3. De rol van de voorzitter
- 4. De vergaderingen
- 5. Evaluatie en beoordeling

De auditcommissie heeft een zware taakstelling, die de afgelopen jaren bovendien sterk is toegenomen in scope en intensiteit. De Code heeft de auditcommissie een kernrol toebedeeld in audit en **control**. Bovendien moet de auditcommissie haar werk doen in een dynamische omgeving. Het accent in (corporate) governance is komen te liggen op meervoudige waardecreatie voor de lange termijn en cultuur, op **hard controls** én **soft controls**, op financiële én niet-financiële informatie.

Verzwarend en verbreding taken en verantwoordelijkheden

Die verschuiving heeft geleid tot een verzwarend en verbreding van de traditionele taken en verantwoordelijkheden van de auditcommissie: het toetsen van de integriteit en de kwaliteit

van de financiële verslaggeving en de effectiviteit van de interne risicobeheersings- en controlesystemen en het toezicht houden op onder meer financiering, ICT & cybersecurity en het belastingbeleid.

Het belang van duurzaamheid voor ondernemingen is bijvoorbeeld enorm toegenomen. Toenemende Europese duurzaamheidsregelgeving heeft een significante invloed op hoe bedrijven opereren en zich positioneren in de markt. Verder kan financiering naast traditionele kredietverlening en kapitaalverstrekking ook fintech-toepassingen omvatten. ICT, GenAI en cybersecurity vormen bewegende doelen door de voortschrijdende digitalisering.

1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Taken en verantwoordelijkheden auditcommissie

volgens de Code (Principe 1.5.1)

De auditcommissie bereidt de besluitvorming van de raad van commissarissen voor over:

- het toezicht op de integriteit en kwaliteit van de financiële- en duurzaamheidsverslaggeving van de vennootschap; en
- de effectiviteit van de interne risicobeheersings- en controlesystemen van de vennootschap.

Daarbij richt de auditcommissie zich onder meer op het toezicht op het bestuur ten aanzien van:

- de relatie met en de naleving van aanbevelingen en de opvolging van opmerkingen van de interne auditor, de externe accountant en indien van toepassing een andere externe partij die betrokken is bij de controle van de duurzaamheidsverslaggeving;
- de financiering van de vennootschap;
- het belastingbeleid van de vennootschap.

Sustainability committee

Inmiddels hebben diverse vennootschappen naast de auditcommissie een commissie ingesteld die zich bezighoudt met duurzaamheidsvraagstukken (ook wel sustainability-commissie of corporate responsibility commissie genoemd). In dat geval kan de voorbereiding van de besluitvorming in het kader van het toezicht op de integriteit en kwaliteit van de duurzaamheidsverslaggeving ook worden uitgevoerd door een dergelijke commissie, in plaats van de auditcommissie.



Wettelijke taak (niet opgenomen in het Besluit-AC) van de auditcommissie volgens de EU-Auditverordening:

- selectie van de externe accountant door middel van een aanbestedingsprocedure.

Wettelijke taken auditcommissie:

volgens het Besluit-AC (artikel 2, lid 2)

- het monitoren van het financiële verslaggevingsproces en het doen van voorstellen om de integriteit van het proces te waarborgen;
- het monitoren van de doeltreffendheid van het interne beheersingssysteem, het eventuele interne auditsysteem en het risicomanagementsysteem met betrekking tot de financiële verslaggeving van de rechtspersoon;
- het monitoren van de wettelijke controle van de jaarrekening en de geconsolideerde jaarrekening, in het bijzonder de uitvoering van de controle met inachtneming van de beoordeling van de Autoriteit Financiële Markten (AFM);
- het beoordelen en monitoren van de onafhankelijkheid van de externe accountant, waarbij met name wordt gelet op de verlening van nevendiensten aan de rechtspersoon;
- het vaststellen van de procedure voor de selectie van de externe accountant en de voordracht tot verlening van de opdracht tot het verrichten van de wettelijke controle.

De invoering van Europese duurzaamheidsregelgeving als de Corporate Sustainability Reporting Directive (CSRD) en de Corporate Sustainability Due Diligence Directive (CSDDD) en de implementatie daarvan in de Nederlandse wet zal ook [of: heeft ook?] gevolgen hebben voor de taken van de auditcommissie inzake het verslaggingsproces rond duurzaamheidsinformatie, zoals opgesomd in het Besluit-AC.

Effectief opereren

De raad van commissarissen moet erop kunnen vertrouwen dat de auditcommissie het uitdijende en dynamische pakket van taken en verantwoordelijkheden goed uitvoert. De werkzaamheden van de auditcommissie vormen immers de basis voor het toezicht en de besluitvorming door de raad. Dat vraagt om een effectief opererende auditcommissie, met een goed begrip van de rol en verantwoordelijkheden van de auditcommissie,

een adequate samenstelling met een effectieve voorzitter, een gedegen werkwijze met de juiste informatievoorziening, efficiënte vergaderingen en voldoende zelfreflectie om het functioneren van de auditcommissie te beoordelen en te verbeteren. Overigens blijven alle leden van de raad van commissarissen verantwoordelijkheid voor de genoemde onderwerpen dragen. De auditcommissie neemt zelf geen besluiten, maar speelt een voorbereidende rol.

1. Het reglement

1. Commissie

1. Het reglement
2. Samenstelling van de auditcommissie
3. De rol van de voorzitter
4. Vergaderingen
5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

De raad van commissarissen stelt een reglement op voor de auditcommissie, waarin de rol en verantwoordelijkheid, de samenstelling en de werkwijze zijn vastgelegd. Het reglement wordt op de website van de organisatie geplaatst, zodat eenieder er kennis van kan nemen. De auditcommissie kan voor haar rol, mandaat en taken naar het reglement verwijzen in het contact met de raad van commissarissen, het management, Internal Audit en de externe accountant. De auditcommissie kan ook op verplichtingen vanuit het reglement worden aangesproken door deze partijen. Aansprakelijkheid van de commissarissen en daarmee de leden van de auditcommissie valt buiten het bestek van deze publicatie.

Blauwdruk voor functioneren en verantwoording

Voor de voorzitter en de leden van de auditcommissie vormt het reglement een vertrek- en ijkpunt voor effectief opereren. Het reglement geeft richting aan het gedrag en de werkzaamheden van de commissie. Zo is het reglement leidend voor de (jaar)agenda van de auditcommissie: welke onderwerpen moet de auditcommissie aanpakken? Daarnaast vormt het reglement een blauwdruk voor de evaluatie van het functioneren en het afleggen van verantwoording in:

- het verslag voor de raad van commissarissen over de belangrijkste beraadslagingen en bevindingen;

- het verslag aan externe stakeholders in het jaarverslag (via het verslag van de raad van commissarissen) over de taakuitvoering. Zie voor de interne en externe verslaglegging ook hoofdstuk 9: Communicatie.



Dynamisch document

Het reglement is geen statisch document, maar ademt mee met aanpassingen van wet- en regelgeving en externe ontwikkelingen. Het is best practice dat de auditcommissie het reglement dan ook ten minste één keer per jaar beoordeelt en eventueel veranderingen voorstelt aan de raad van commissarissen.

Bijlage 1B biedt een overzicht van belangrijke aandachtspunten voor een reglement.



Wat staat er in het reglement?

Het reglement van de auditcommissie bevat de volgende onderwerpen:

- doelstellingen;
- mandaat en bevoegdheden;
- rol en verantwoordelijkheden
- omvang;
- samenstelling: hoofd- en nevenfuncties, kwalificaties, benoemingsperiode en zittingsduur;
- vergaderingen: frequentie, deelnemers, informatie en rapportages;
- relatie met het bestuur, Internal Audit en de externe accountant;
- zelfevaluatie van de auditcommissie;
- rapportage;
- bevoegdheid om – indien gewenst – bijzondere onderzoeken uit te voeren.

Aandachtspunten bij het reglement

- Hoever reikt de verantwoordelijkheid van de auditcommissie voor risicomanagement, **compliance** en interne controle: het gehele risicomanagementsysteem of alleen de financiële risico's?
- Is er sprake van een **risk committee** (veelal in de financiële sector) en wat is de relatie ten opzichte van de auditcommissie?
- Heeft de auditcommissie specifieke verantwoordelijkheden op zich genomen, zoals de beoordeling van de governancestructuur van de organisatie?
- Biedt het reglement voldoende flexibiliteit om de auditcommissie in staat te stellen effectief te opereren, terwijl rollen en verantwoordelijkheden tegelijkertijd helder zijn geformuleerd?
- Geeft het reglement de auditcommissie toegang tot de mensen en middelen, de informatie en de onafhankelijke advisering die de commissie nodig heeft om aan de verplichtingen te voldoen?



2. Samenstelling van de auditcommissie

- 1. Commissie
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
 - 4. Vergaderingen
 - 5. Evaluatie van de auditcommissie
 - Bijlagen
- 2. Continuïteit
 - 3. Corporate impact
 - 4. Control & Compliance
 - 5. Cultuur en gedrag
 - 6. Checks & Balances
 - 7. Corporate Reporting
 - 8. Crisis
 - 9. Communicatie

De kwaliteit en effectiviteit van de auditcommissie staat of valt met de samenstelling van de commissie. De leden van de auditcommissie zijn afkomstig uit de raad van commissarissen en worden door de raad van commissarissen benoemd. Commissarissen moeten beschikken over de benodigde deskundigheid, achtergrond, competenties en onafhankelijkheid om hun taken naar behoren te vervullen. Dat geldt dus ook voor de leden van de auditcommissie.

Daarnaast geldt een aantal aanvullende eisen voor leden van de auditcommissie, neergelegd in de wet en de Code.

Wettelijke eisen samenstelling auditcommissie

De auditcommissie is samengesteld uit leden van de raad van commissarissen of uit leden van het bestuur die niet belast zijn met het uitvoerend bestuur.

- Bij de samenstelling van de auditcommissie wordt rekening gehouden met de benodigde deskundigheid van de leden gezamenlijk die relevant is voor de sector waarin de rechtspersoon actief is.
- De meerderheid van de leden, waaronder de voorzitter, is onafhankelijk van de rechtspersoon. (Deze eis is ook opgenomen in de Code, alleen wordt de onafhankelijkheid van de voorzitter daar niet expliciet genoemd.)
- Ten minste één lid is deskundig op het gebied van (niet-)financiële verslaggeving of de controle van de jaarrekening en het sustainability statement (CSRD).
- De voorzitter wordt benoemd door de raad van commissarissen of door de leden van het bestuur die niet belast zijn met het uitvoerend bestuur dan wel door de leden van de auditcommissie.

Profiel voor leden van de auditcommissie

Om voor de auditcommissie in aanmerking te komen, moeten leden over de juiste combinatie van kennis, ervaring, competenties, eigenschappen en houding beschikken. Het is gebruikelijk dat de raad van commissarissen een profielschets opstelt en deze op de website publiceert. Deze profielschets is leidend voor rekrutering van nieuwe leden voor de raad van commissarissen dan wel de auditcommissie.

Deskundigheid op het gebied van verslaggeving

Expertise op het gebied van verslaggeving in de auditcommissie is cruciaal. Ten minste één lid beschikt over deze expertise. Veiliger is als de auditcommissie over twee verslaggevingsexperts

beschikt, mocht er een van hen plotseling terugtreden, of ter overbrugging bij opvolging. Overigens worden ook de andere leden van de auditcommissie geacht over voldoende (niet-)financiële kennis te beschikken. Zo moeten alle leden in staat te zijn om een jaarverslag, bestaande uit een jaarrekening (de balans, de winst-en-verliesrekening en het kasstroomoverzicht) en een sustainability statement, te lezen en te begrijpen, daarover relevante vragen te stellen, de antwoorden te interpreteren en eventueel door te vragen (zie bijlage 1C).

Deskundigheid op het gebied van duurzaamheid

Ook kennis van niet-financiële en niet-kwantitatieve aard mag niet ontbreken, gezien de EU-duurzaamheidsregelgeving en het accent op langetermijnwaardecreatie en cultuur in hedendaagse governance. Door de wijziging van het Besluit-AC ten gevolge van de EU-duurzaamheidsregelgeving, behoort ook toezicht op de kwaliteit en integriteit van de duurzaamheidsverslaglegging tot de taken van de auditcommissie. Alhoewel het nu (nog) niet wettelijk verplicht is, is het wel aan te raden om ook een deskundige op het gebied van duurzaamheidsrapportage aan de auditcommissie toe te voegen.

Diversiteit leidt tot verrijking

Kennis en expertise op het gebied van financiën en duurzaamheid is echter niet voldoende om het gehele pakket aan taken en verantwoordelijkheden

van de auditcommissie af te dekken. Eveneens onmisbaar is kennis van de sector waarin de organisatie actief is, en expertise op het gebied van risicomanagement, cybersecurity, privacy en (gen) AI.

Het gaat verder niet alleen om hard controls, maar ook om soft controls. Zachte vaardigheden in de auditcommissie – zoals empatisch vermogen, teamwork, probleemoplossing en communicatie – kunnen een positieve bijdrage leveren aan de relatie van de auditcommissie met het bestuur, het management, Internal Audit en de externe accountant.

Juist de inbreng vanuit verschillende expertises, invalshoeken of achtergronden leidt tot verrijking van de discussie. De auditcommissie moet dus divers zijn samengesteld, waarbij ook het diversiteits- en inclusiebeleid van de vennootschap in acht wordt genomen.

Onafhankelijkheid in positie

De criteria voor onafhankelijkheid van de auditcommissie zijn gelijk aan die voor de overige leden van de raad van commissarissen. Het gaat om onafhankelijkheid in positie. De meerderheid van de leden van de auditcommissie mag onder meer:

- geen werknemer of bestuurder van de organisatie zijn geweest in de voorafgaande vijf jaar;
- geen persoonlijke vergoeding hebben ontvangen (anders dan voor de toezichtpositie);

- 1. Commissie
 - 1. Het reglement
- 2. Samenstelling van de auditcommissie
- 3. De rol van de voorzitter
- 4. Vergaderingen
- 5. Evaluatie van de auditcommissie
- Bijlagen

- 2. Continuïteit

- 3. Corporate impact

- 4. Control & Compliance

- 5. Cultuur en gedrag

- 6. Checks & Balances

- 7. Corporate Reporting

- 8. Crisis

- 9. Communicatie

- geen zakelijke relatie hebben gehad (of het kantoor waar hij of zij werkzaam was) in het voorafgaande jaar. Bij een OOB moet er twee jaar verstreken zijn voor de accountant die betrokken was bij de wettelijke controle of de voornaamste vennoot was van het betrokken kantoor, kan toetreden tot de auditcommissie.

Geestelijke onafhankelijkheid
Het gaat niet alleen om onafhankelijkheid in positie, maar ook om geestelijke onafhankelijkheid. Van leden van de auditcommissie worden de juiste competenties en houding verwacht:

- **Gezonde scepsis, nieuwsgierigheid en autonoom oordeelsvermogen**

Leden van de auditcommissie willen hun intellectuele nieuwsgierigheid bevredigen, zijn bedreven in het stellen van kritische vragen en in doorvragen en zijn onvermoeibaar in het zoeken naar aanvullende informatie als ze ontevreden zijn met de informatie van het bestuur, het management of andere betrokkenen. Daarbij gebruiken ze hun ervaring, intuïtie en onafhankelijk oordeel.

- **Integriteit en een rechte rug**
- Leden van de auditcommissie hebben een rechte rug om de toon aan de top te ondersteunen en het bestuur en het management aan te spreken op hun gedrag. Ze beschikken over autoriteit en moreel overwicht bij hun medecommissieleden, het bestuur en het management. In een crisissituatie – waarbij de auditcommissie een onderzoek naar de gang van zaken uitvoert – zijn integriteit,

objectiviteit en een rechte rug nog belangrijker.

Voldoende tijd beschikbaar hebben
Voor een benoeming tot lid van de auditcommissie geldt ook een praktische voorwaarde: voldoende tijd kunnen besteden aan de commissie. Het lidmaatschap van de commissie brengt veel leeswerk en extra vergaderingen met zich, de materie is complex en het pakket aan taken en verantwoordelijkheden wordt steeds breder en zwaarder. Bij de selectie van de leden van de auditcommissie zal dan ook gekeken worden naar de eventuele hoofdfunctie, plus het aantal commissariaten en commissielidmaatschappen dat kandidaten elders vervullen.

Omvang van de auditcommissie
Een auditcommissie moet groot genoeg zijn om een goede balans te kunnen vinden tussen verschillende inzichten en ervaringen, maar ook klein genoeg om efficiënt te kunnen functioneren. In Nederland is een auditcommissie van twee tot vier leden het meest gebruikelijk. De ideale omvang van de auditcommissie hangt af van de omvang van de volledige raad van commissarissen, de specifieke omstandigheden en uitdagingen van de organisatie en daarmee de verantwoordelijkheden van de auditcommissie.

Zittingsperiode leden auditcommissie
Bij het bepalen van de benoemingsperiode van de commissieleden moeten twee factoren tegen elkaar worden afgewogen, te weten: continuïteit en vernieuwing. Omwille van de continuïteit heeft een benoemingsperiode voor meerdere jaren de

- Van leden van de auditcommissie mag het volgende worden verwacht:**
- integriteit;
 - geestelijke onafhankelijkheid en nieuwsgierigheid;
 - kritische instelling en vermogen om door te vragen;
 - in staat zijn direct en eerlijk een eigen mening te geven;
 - vermogen om nieuwe of afwijkende inzichten en constructieve suggesties in te brengen;
 - financiële expertise.

Beperking aantal lidmaatschappen auditcommissie
De New York Stock Exchange eist dat commissarissen die bij meer dan drie beursgenoteerde ondernemingen zitting hebben in de auditcommissie daarvoor toestemming hebben gekregen van elk van de betrokken boards.

Tijdsbeslag versus kruisbestuiving
In Nederland maximeert de Wet bestuur en toezicht het aantal toezichtposities bij grote rechtspersonen tot vijf, waarbij voorzitterschappen dubbel tellen. De wet weegt voorzitterschappen of lidmaatschappen van (audit)commissies niet extra mee. Een ‘stapeling’ van deze posities bij leden van de auditcommissie zou echter een te groot tijdsbeslag kunnen vormen, zeker voor voorzitters. Anderzijds kan het een meerwaarde zijn wanneer leden van de auditcommissie vaker dezelfde positie bekleden: het commissiewerk voor andere bedrijven fungeert als benchmark en zorgt voor kruisbestuiving en het up-to-date houden van kennis. Het is dus zoeken naar de juiste balans.

voorkeur. Op die manier kan kennis en ervaring worden opgebouwd en kan de commissie daarvan optimaal profiteren. Aan de andere kant kunnen te lange zittingstermijnen leiden tot verlies van scherpste en onafhankelijkheid ten opzichte van het bestuur en het management. Herbenoeming voor een nieuwe termijn zal dan ook zorgvuldig overwogen dienen te worden.

Rouleren tussen commissies
Nieuwe leden kunnen een frisse kijk op de gang van zaken inbrengen en de effectiviteit van de auditcommissie vergroten. Het rouleren van de commissarissen over de verschillende commissies is daarvoor een beproefde methode. Daarnaast is het van belang om tijdens de jaarlijkse evaluatie te kijken naar de

1. Commissie

1. Het reglement
2. Samenstelling van de auditcommissie
3. De rol van de voorzitter
4. Vergaderingen
5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

samenstelling van de auditcommissie en de vraag te stellen welke kennis en ervaring kan worden aangevuld of ververst. Zeker nu ook thema's als langetermijnwaardcreatie en de monitoring van cultuur worden geadresseerd en zowel niet-financiële als kwalitatieve expertise vereist is. De uitkomst van de evaluatie kan aanleiding zijn tot wijzigingen in de bezetting.

Opvolgingsplanning

Ook goede opvolgingsplanning voor de auditcommissie is van belang. Het is zaak te voorkomen dat te veel leden tegelijk aftreden. Een groot verloop kan nadelig zijn voor de continuïteit en daarmee voor de effectiviteit van de commissie: nieuwe leden hebben tijd nodig om inzicht te krijgen in de activiteiten van een organisatie en om specifieke vraagstukken te doorzien. Denk dus tijdig na over de opvolging van zittende leden. Eventueel kan de omvang van de auditcommissie ter overbrugging worden uitgebreid, door (tijdelijke) herbenoeming van ervaren leden die hun opvolgers kunnen inwerken.

Inwerken nieuwe leden van de auditcommissie

Nieuwe leden van de auditcommissie volgen evenals andere nieuwe commissarissen een introductieprogramma. Nieuwe leden van de auditcommissie zullen bovendien additionele behoefte hebben aan financieel georiënteerde en duurzaamheidsgeoriënteerde kennis van de organisatie (indien toezicht op duurzaamheidsrapportage onderdeel is van de taken van de auditcommissie), om snel



‘Onboarding’

Tijdens het inwerken van nieuwe leden van de auditcommissie wordt aandacht besteed aan:

- de eisen en doelstellingen van de auditcommissie;
- het auditcommissiereglement;
- de verwachte tijdsbesteding door de commissieleden;
- een overzicht van de bedrijfsactiviteiten;
- de notulen van vorige vergaderingen;
- recente rapporten die de auditcommissie aan de raad van commissarissen heeft uitgebracht (zie bijlage 1D voor een uitgebreider overzicht).

meerwaarde te kunnen leveren. Succesvolle onboarding voor leden van de auditcommissie begint veelal met een gesprek met de voorzitter en omvat verder gesprekken met de ceo, de cfo en leden van de financiële kolom, Internal Audit en de externe accountant. Op die manier wordt een dieper inzicht verkregen in de financiële rapportage, de duurzaamheidsrapportage, de risicogebieden en de interne risicobeheersings- en controlesystemen.

Best practice

Laat nieuwe commissarissen als toehoorder aanschuiven bij de auditcommissie. Meeluisteren naar de discussie over de zaken die op de agenda staan van de auditcommissie (zoals zicht op risico's, financiële verslaggeving, schattingen) is waardevol en een efficiënte manier om nieuwe commissarissen in te werken en op te leiden – zelfs als ze geen lid van de auditcommissie worden.

Ook na de **onboarding** is het ontvangen van stukken voor de auditcommissie en een staande uitnodiging voor het bijwonen van de vergadering van de auditcommissie best practice.



3. De rol van de voorzitter

- 1. Commissie
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
 - 4. Vergaderingen
 - 5. Evaluatie van de auditcommissie
 - Bijlagen
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Een effectieve auditcommissie begint met een goede voorzitter. Hij of zij fungeert als de verbinding voor de relaties van de auditcommissie met de raad van commissarissen, de cfo, het (financieel) management, Internal Audit en de externe accountant en optimaliseert de samenwerking. Daarnaast stelt de voorzitter de agenda op en zorgt hij of zij voor het soepel verlopen van de vergadering. De voorzitter let erop dat alle leden voldoende aan bod komen en koppelt terug naar de voltallige raad van commissarissen. Hij of zij stemt zo nodig ook af met andere commissies in de raad van commissarissen, zoals met de remuneratiecommissie, **risk committee** en **sustainability committee**.

Voorzitterschap vraagt specifieke competenties

Goede voorzitters beschikken niet alleen over de juiste inhoudelijke kennis en behendigheid in het leiden van vergaderingen, maar kunnen ook goed luisteren, hebben een antenne voor non-verbale signalen en weten onderlinge dynamiek in goede banen leiden. Ze hebben ook de moed om leden aan te spreken op hun inbreng of opstelling binnen de commissie.

Geen dubbel voorzitterschap

Het voorzitterschap van de audit- of remuneratiecommissie mag niet worden vervuld door de voorzitter van de raad van commissarissen of door een voormalig bestuurder van de organisatie. Beide voorzitterschappen zijn intensief: een combinatie zou tot een te zware belasting leiden. Bovendien kan een

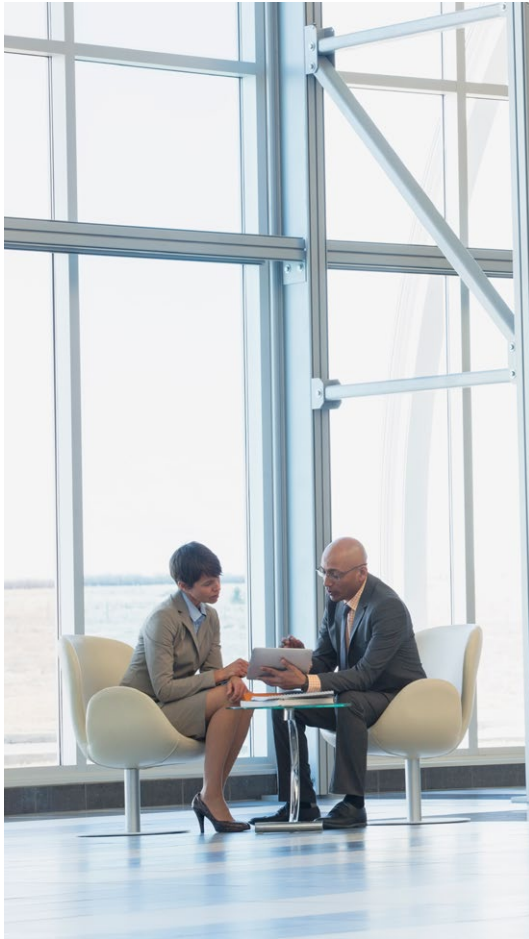
dubbel voorzitterschap gevolgen hebben voor de dynamiek. Voor een raad van commissarissen zou het moeilijk kunnen zijn om een voorstel van de auditcommissie niet te volgen, wanneer het voorzitterschap van de commissie wordt vervuld door de voorzitter van de raad van commissarissen. Dat zou een evenwichtige besluitvorming door de raad van commissarissen op het gebied van de financiële verslaggeving kunnen doorkruisen.

Overweeg om de rol van voorzitter en financieel/duurzaamheidsexpert te scheiden

In de praktijk zien we dat de voorzitter van de auditcommissie vaak ook de rol van financieel expert vervult. Het is te overwegen om deze twee rollen niet te laten samenvallen. Dat kan de balans van vaardigheden binnen de commissie ten goede komen. De voorzitter moet door de financieel expert dan wel goed op de hoogte worden gebracht van de financieel-technische aspecten om deze aan de raad van commissarissen en de aandeelhouders te kunnen rapporteren. Als de voorzitter wel zelf de financieel expert is, moet deze ervoor waken de

discussie te domineren met zijn of haar financiële kennis. Hetzelfde is van toepassing indien de voorzitter van de auditcommissie de rol van duurzaamheidsexpert vervult.

Welke karakteristieken zorgen voor een sterke voorzitter van de auditcommissie?



1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Tips voor de rol van voorzitter:

- Wees proactief – besluit wat u wilt doen, plan, en neem de leiding.
- Zorg voor een goed tijdschema zodat de auditcommissie zaken op tijd onder ogen krijgt.
- Zorg dat de agenda op orde is zodat de leden zich voor kunnen bereiden en de vergaderingen effectief verlopen.
- Ken de sterktes en zwaktes van de leden.
- Zorg ervoor dat de raad goed geïnformeerd is – zowel mondeling als door middel van de notulen.
- Trek nauw op met de cfo (en met degene die (eind) verantwoordelijk is voor de duurzaamheidsverslaggeving, indien dit bij iemand anders dan de cfo is belegd). om er zeker van te zijn dat jullie elkaar op tijd informeren over relevante zaken.
- Laat de bestuurssecretaris een ondersteunende rol spelen bij de uitvoering van deze taken.
- Leer de externe accountant kennen zodat u op effectieve wijze kunt sonderen, de relatie met het management leert begrijpen, en alert kunt zijn op mogelijke problemen.
- Zorg dat de leden op de hoogte blijven van de verslagleggingsstandaarden (zowel financieel als op het gebied van duurzaamheid) en ontwikkelingen op het gebied van regelgeving.
- Zorg ervoor dat interne controlezaken volledig besproken worden met het bestuur, de interne auditor en de externe accountant, en dat de issues op tafel komen.
- Zorg voor een directe lijn met de interne controleafdeling (Internal Audit) en begrijp wat ze doen.
- Gebruik de rol om communicatie met de financiële markt te stimuleren.
- Zorg voor een flexibele auditcommissie – niet gehinderd door routines.



- 1. **Commissie**
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
- 4. **Vergaderingen**
 - 5. Evaluatie van de auditcommissie
 - Bijlagen
- 2. **Continuïteit**
- 3. **Corporate impact**
- 4. **Control & Compliance**
- 5. **Cultuur en gedrag**
- 6. **Checks & Balances**
- 7. **Corporate Reporting**
- 8. **Crisis**
- 9. **Communicatie**

4. Vergaderingen

De vergaderingen van de auditcommissie vormen het platform voor dialoog en discussie over de kwaliteit en integriteit van de verslaggeving, compliance en risicobeheer: onderling en met de betrokkenen binnen en buiten de organisatie. Een goede dialoog vraagt om goede organisatie: vergaderingen die ruim van tevoren worden gepland en goed worden geleid, met een zorgvuldig opgestelde agenda – afgeleid van het reglement en de jaaragenda – en compact leesmateriaal dat tijdig wordt verspreid.

Planning van de vergaderingen
Auditcommissies in Nederland vergaderen gemiddeld vier tot zes keer per jaar. Het behalen van de doelstellingen van de auditcommissie is maatgevend voor de frequentie, dus er kan ook vaker worden vergaderd, als dat noodzakelijk is. Bij een crisis zal het aantal vergaderingen snel oplopen. In het verlengde van de reguliere vergaderingen van de auditcommissie, zijn er één of meer aparte sessies met de cfo, Internal Audit en de externe accountant, de zogenoemde **private sessions**.

Plan ver vooruit
Vergaderingen van de auditcommissie moeten ver vooruit gepland worden, het is gebruikelijk deze soms wel één tot twee jaar vooruit te plannen. De agenda's van de voorzitter en de leden lopen immers vaak vol, zeker als elders ook commissariaten worden bekleed, al of niet met een lidmaatschap van de auditcommissie. Bovendien kan de vergadering worden bijgewoond door anderen, zoals de cfo (degene

die degene die verantwoordelijk is voor de urzaamheidsverslaggeving, (het hoofd) Internal Audit, de externe accountant en (op uitnodiging) de ceo.

Koppel vergaderplanning aan de jaarcyclus
Efficiënt is om de vergaderplanning van de auditcommissie synchroon te laten lopen met:
1. de (strategische) planning-en-controlcyclus;
2. de interne verslaglegging;
3. het controleproces van Internal Audit en de externe accountant;
4. de externe kwartaalberichtgeving (indien van toepassing);
5. het vergaderschema van de raad van commissarissen

Plan vergaderingen ruim voor de commissarissenvergadering
Vergaderingen van de auditcommissie worden bij voorkeur geruime tijd voor de commissarissenvergadering gepland. Op die manier kan de voorzitter van de auditcommissie schriftelijk verslag uitbrengen aan de raad van commissarissen over de vergadering van de commissie. Dat geeft de overige commissarissen de gelegenheid om het verslag grondig te lezen en er eventueel tijdens de commissarissenvergadering op te reageren.

In de praktijk wordt er soms voor gekozen om de vergadering van de auditcommissie direct voorafgaand aan de vergadering van de raad van commissarissen te laten plaatsvinden, om ook buitenlandse commissarissen in staat te stellen de

vergadering bij te wonen. Er wordt dan mondeling verslag uitgebracht, eventueel later gevolgd door een schriftelijk verslag (zie voor de inhoud van het verslag en het informeren van de raad van commissarissen hoofdstuk 9: Communicatie).

Stuur andere commissarissen tijdig de notulen en het verslag
Ook de notulen van de vergadering van de auditcommissie – in aanvulling op het verslag van de voorzitter – worden tijdig verstuurd

aan de leden van de commissie en de raad van commissarissen. De notulen en het verslag helpen om de commissarissen tussentijds op de hoogte en betrokken te houden en kunnen daarmee een informatiekloof tussen de auditcommissie en de raad van commissarissen voorkomen.



Best practices voor de agenda

Wijs een contactpersoon vanuit het management aan – de auditcommissie heeft hulp nodig bij het opstellen van de agenda, inclusief wijzigingen die zich gedurende het jaar voordoen. Het is belangrijk om een specifiek persoon aan te wijzen (bijvoorbeeld de bestuurssecretaris, of de controller) om samen met de overige managementleden op te trekken en aanpassingen van de agenda te coördineren.

Voldoe aan het reglement – het reglement van de auditcommissie is het startpunt voor het plannen van de agenda voor komend jaar. Het reglement is de toezegging die de auditcommissie heeft gedaan aan de aandeelhouders en geeft weer welke acties zij moet uitvoeren. Ieder onderdeel uit het reglement moet op de agenda worden gezet.

Plan aan het begin van het jaar de onderwerpen voor het hele jaar vooruit – zowel de onderwerpen op de agenda als de tijd die ervoor beschikbaar is – voor alle geplande vergaderingen. De meeste onderwerpen komen iedere keer terug. Reserveer ook tijd voor diepgaandere discussies over geselecteerde onderwerpen, zoals IT of belastingen. En laat ook tijd over voor onverwachte zaken die gedurende het jaar op kunnen komen.

Bevestig de onderwerpen op de agenda voordat de vergadering begint – een essentiële stap voor de voorzitter van de auditcommissie is om de agenda af te stemmen met de andere commissieleden, het management en de externe accountant voordat de agenda wordt rondgestuurd. De voorzitter kan dan nog wijzigingen aanbrengen in de onderwerpen of de tijd die is toebedeeld per onderwerp.

- 1. **Commissie**
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
- 4. **Vergaderingen**
 - 5. Evaluatie van de auditcommissie
 - Bijlagen
- 2. **Continuïteit**
- 3. **Corporate impact**
- 4. **Control & Compliance**
- 5. **Cultuur en gedrag**
- 6. **Checks & Balances**
- 7. **Corporate Reporting**
- 8. **Crisis**
- 9. **Communicatie**

Vraag als voorzitter om agendasuggesties aan andere leden

De vergaderagenda wordt opgesteld door de voorzitter, geassisteerd door de bestuurssecretaris. De voorzitter vraagt voorafgaand aan elke vergadering of de andere leden van de commissie nog suggesties hebben voor te bespreken onderwerpen. De agenda kan per onderwerp een tijdsindicatie bevatten (maar durf daarvan af te wijken) en de bijdrage die van de leden van de commissie wordt gevraagd: goedkeuring van een besluit, advies of slechts kennisneming? Dezelfde ‘legenda’ kan gelden voor de vergaderstukken.

Informatievoorziening

De auditcommissie wordt geacht voorafgaand aan de vergadering in korte tijd veel informatie door te nemen. Voorzitters en leden van de auditcommissie vinden vaak dat het om te veel informatie gaat, die soms ook nog eens te laat wordt aangeleverd. Ze hebben ook behoefte aan toegankelijker informatie: meer inzichten van het management, de belangrijkste risico’s uitgelicht, visualisering en meer samenvattingen. Daarvoor kan ook een beroep worden gedaan op de bestuurssecretaris. Hij of zij kan een regisseursrol vervullen en ervoor zorgen dat de commissie tijdig goed gedoseerde, gerichte en goed ontsloten informatie ontvangt. De voorzitter kan na lezing van de vergaderstukken ook contact leggen met bijvoorbeeld de cfo (en degene die verantwoordelijk is voor de duurzaamheidsverslaggeving), de controller, Internal Audit of de externe accountant om alvast een toelichting te vragen en feedback te geven,



Best practices voor de agenda



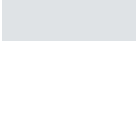
Stem de timing af – de leden van de commissie hebben tijd nodig om de stukken te lezen en te verwerken. Doorgaans streeft het management ernaar om de stukken minimaal één week voor de vergadering beschikbaar te hebben. Een kortere voorbereidingstijd kan goed zijn voor telefonische vergaderingen met een beperkte agenda, zoals het publiceren van de kwartaalcijfers. Nu het gebruik van portals gemeengoed is geworden, kunnen de stukken het beste op een portal worden geplaatst zodra ze beschikbaar zijn, maar zorg ervoor dat de deadlines voor de belangrijkste onderwerpen helder zijn.



Zorg voor samenvattingen – leden van auditcommissies hebben vaak last van een overload aan informatie. Een goede samenvatting van alle onderdelen van de stukken die van tevoren worden gelezen kan helpen. Een effectieve commissie zorgt voor een protocol met het bestuur waarbij de schriftelijke stukken beginnen met de conclusie en de benodigde diepgang volgt in de rest van de documentatie. Gebruikelijke aandachtspunten voor goede samenvattingen zijn: waarom het onderwerp is aangepakt, inzichten en conclusies van het bestuur, key takeaways, te nemen acties en tijdlijnen.



Markeer veranderingen – het doornemen van het grote aantal terugkerende stukken die bij de toezichthouder moeten worden gedeponneerd, diverse rapporten van het bestuur en de communicatie van externe accountants kan een behoorlijke uitdaging zijn. Veel van de rapporten die vaak terugkomen, bevatten nagenoeg dezelfde woorden, dit maakt het lastig om te beoordelen wat nieuwe informatie is of wat er veranderd is ten opzichte van de vorige vergadering. Verzoek het management daarom om substantiële veranderingen ten opzichte van het vorige kwartaal in deze rapporten te markeren. Dit stelt de auditcommissie in staat om zich te focussen op de onderliggende oorzaak van de veranderingen, met name wanneer deze onverwacht waren.



Gebruik bijlagen – de verschillende leden van de commissie hebben mogelijk verschillende behoeften voor wat betreft diepgang in de materie. Door te focussen op de kern en de ‘nice-to-have’ details in een bijlage op te nemen, worden de stukken beknopter en gerichter, zonder dat dit ten koste gaat van degenen die meer willen lezen. Zorg ervoor dat alle commissieleden overeenstemming hebben over de gewenste mate van detail in de bijlagen. Het kan voorkomen dat commissieleden het juridische team van de organisatie willen consulteren om zich ervan te vergewissen wat hun verplichting is, mocht dit van toepassing zijn, om de aanvullende informatie in de bijlagen tot zich te nemen.

om de vergadering efficiënter en soepeler te laten verlopen.

Haal- en brengplicht

Overigens mag de auditcommissie bij de informatievoorziening niet alleen afgaan op de brengplicht van het bestuur, de leden hebben ook een haalplicht: het proactief op zoek gaan naar onafhankelijke informatie(bronnen), in aanvulling op en ter controle van de informatie van het bestuur. Zie daarvoor ook hoofdstuk 9: Communicatie.

Bijwonen van de vergadering

Het spreekt vanzelf dat de voorzitter en de leden van de auditcommissie worden geacht om alle vergaderingen bij te wonen. Bij frequente afwezigheid worden de betrokken leden daarop aangesproken. Het aanwezigheidspercentage van elk lid van de auditcommissie bij de vergaderingen wordt vermeld in het verslag van de raad van commissarissen (net als het aantal vergaderingen en de belangrijkste besproken onderwerpen).

- 1. Commissie
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
 - 4. Vergaderingen
 - 5. Evaluatie van de auditcommissie
 - Bijlagen
- 2. Continuïteit
 - 3. Corporate impact
 - 4. Control & Compliance
 - 5. Cultuur en gedrag
 - 6. Checks & Balances
 - 7. Corporate Reporting
 - 8. Crisis
 - 9. Communicatie

Aanwezigen bij de vergadering van de auditcommissie



Ceo wel of niet bij de vergadering?
Naast de leden van de auditcommissie worden de vergaderingen bijgewoond door de cfo (en degene die verantwoordelijk is voor de duurzaamheidsverslaggeving), (het hoofd) Internal Audit en de externe accountant, tenzij de auditcommissie anders bepaalt. De auditcommissie bepaalt ook of en wanneer de voorzitter van het bestuur bij haar vergaderingen aanwezig is. Doorgaans wil de commissie de

cfo, plus degene die verantwoordelijk is voor de duurzaamheidsverslaggeving (en eventueel de ceo op uitnodiging) de gelegenheid geven om vrijuit te spreken, zonder aanwezigheid van de ceo. Soms schuift de ceo (op verzoek van de commissie) wel aan bij de bespreking van de eventuele kwartaalcijfers, de halfjaarcijfers en de jaarrekening. Het is best practice dat de interne auditor en de externe accountant alle vergaderingen van de auditcommissie bijwonen.

Tweede echelon, staf en externe deskundigen uitnodigen

De auditcommissie kan ook andere managers of staffunctionarissen uitnodigen voor (een deel van) de vergadering, zoals de chief risk officer, compliance officer, general counsel, chief information officer/chief digital officer, chief sustainability officer, director Tax, et cetera. of chief sustainability officer, director Tax et cetera. Ook deelname van externe deskundigen, zoals een juridisch adviseur, behoort tot de mogelijkheden. Wel moet dit vooraf zijn overlegd met het bestuur. (Zie bijlage 1F voor een overzicht van de aanwezigheid en mogelijke bijdrage van andere deelnemers aan de vergadering van de auditcommissie).

Aanwezigheid andere commissarissen

Verder kunnen ook de andere commissarissen de vergaderingen van de auditcommissie bijwonen. Sommige raden van commissarissen plannen vergaderingen van de diverse commissies bewust niet tegelijk in, om commissarissen in staat te stellen deze bij te wonen. Als de vergadering van de auditcommissie vlak voor de commissarissenvergadering plaatsvindt, maken buitenlandse commissarissen vaak van deze gelegenheid gebruik om ‘bijgepraat’ te worden. Voor nieuwe commissarissen is het bijwonen van de vergadering van de auditcommissie een efficiënte manier om zich in te werken in hun toezichtfunctie.

Beperk het aantal deelnemers

Het voordeel van interne of externe deelnemers bij de vergadering van de auditcommissie is dat vragen van de commissie direct beantwoord kunnen worden. Wanneer het gezelschap echter te groot wordt, ligt inefficiency op de loer. Ook kunnen leden van de auditcommissie terughoudend zijn in het stellen van vragen, als ze in de minderheid zijn, of kunnen managers of staffunctionarissen het lastig vinden om vrijuit te praten in aanwezigheid van hun meerdere of collega’s.

- 1. Commissie
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
 - 4. Vergaderingen
 - 5. Evaluatie van de auditcommissie
 - Bijlagen
- 2. Continuïteit
 - 3. Corporate impact
 - 4. Control & Compliance
 - 5. Cultuur en gedrag
 - 6. Checks & Balances
 - 7. Corporate Reporting
 - 8. Crisis
 - 9. Communicatie

Best practice executive en private sessions

‘Executive sessions’

Aanwezigen:

Alleen de leden
van de auditcommissie

Doel:

Het bevorderen van openhartige en
vertrouwelijke gesprekken buiten de
formele vergaderstructuur

Frequentie:

Aan het begin en het einde van de
meeste, zo niet alle, vergaderingen

‘Private sessions’

Aanwezigen:

In ieder geval de cfo, de interne auditor
en de externe accountant; waarbij
eenieder van hen de mogelijkheid
moet hebben om ook alleen een
private session te hebben met de
commissie. Wellicht willen ook het
hoofd Compliance en het hoofd Risk een
sessie, of een van de anderen die af en
toe aanwezig zijn op de vergaderingen,
zoals het hoofd IT-beveiliging,
het hoofd Informatie of de fiscaal
verantwoordelijke.

Doel:

- het bevorderen van openhartige en
vertrouwelijke gesprekken in een
ongestructureerde omgeving;
- het bouwen aan relaties;
- het verduidelijken van onderwerpen
die in de ‘grote’ vergadering aan de
orde zijn geweest;
- het bespreken van gevoelige
onderwerpen, bijvoorbeeld het risico
op fraude of de bedrijfscultuur;
- het mentoren en coachen van leden
van het bestuur; de gezamenlijke
kennis en ervaring van de
auditcommissie is immers zeer
waardevol en moet ingezet worden
om de leden van het bestuur te
ondersteunen in hun ontwikkeling.

Frequentie:

Aan het eind van alle
face-to-face vergaderingen

‘Executive sessions’

Voorafgaand en na afloop van de vergadering van de auditcommissie hebben de voorzitter en de leden apart overleg met elkaar: **executive sessions** genoemd. Bij de voorbespreking kan er gereageerd worden op de stukken en een laatste toevoeging aan de agenda worden gedaan. Bij de nabespreking kunnen prioriteiten worden bepaald en kan alvast oriënterend naar de agenda voor de volgende keer worden gekeken.

‘Private sessions’

De auditcommissie heeft ook regelmatig vergaderingen waarin een-op-een wordt gesproken met interne en externe partijen: de zogenoemde **private sessions**. Zo overlegt de auditcommissie ten minste eenmaal per jaar, buiten aanwezigheid van het bestuur, met de externe accountant (en daarnaast zo vaak als de commissie nodig vindt). Ook heeft de auditcommissie direct toegang tot (het hoofd) Internal Audit. Verder kan apart worden overlegd met de cfo (en degene die verantwoordelijk is voor de duurzaamheidsverslaggeving), of andere managers en staffunctionarissen. Ook geldt het omgekeerde: er kan om een een-op-eengesprek met de auditcommissie gevraagd worden.

Thema’s te bespreken in ‘private sessions’

Het voordeel van een private session is het vrijelijk kunnen bespreken van (gevoelige) onderwerpen, bijvoorbeeld de samenwerking binnen het bestuursteam zoals beleefd door de cfo. Onderwerpen van het gesprek met de interne auditor dan wel de externe accountant kunnen bijvoorbeeld zijn: de kwaliteit van de cfo en de financiële kolom, of het leggen van oneigenlijke financiële druk op de organisatie. Daarnaast lenen private sessions zich ook goed voor het delen en toetsen van signalen van mogelijke integriteitsrisico’s of een ongezonde cultuur die om alertheid of nader onderzoek vragen. Zie voor een uitgebreide bespreking van private sessions hoofdstuk 6, over de relatie met Internal Audit en de externe accountant.

5. Evaluatie van de auditcommissie

1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

De auditcommissie moet het eigen functioneren ten minste één keer per jaar beoordelen, net als de raad van commissarissen waar de commissie deel van uitmaakt. Dat kan plaatsvinden door zelfevaluatie, of onder externe begeleiding. Een externe begeleider is als buitenstaander onafhankelijk, objectief en onbevooroordeeld en kan gemakkelijker gevoelige onderwerpen en de onderlinge dynamiek aanpakken. Een externe evaluatie – jaarlijks of bijvoorbeeld eens in de drie jaar – is daarmee het meest effectief.

Permanente evaluatie

Daarnaast kan de auditcommissie na elke vergadering het eigen functioneren kort onder de loep nemen, bijvoorbeeld tijdens de executive session: hoe verliep de vergadering, wat was de kwaliteit van de discussie, hoe was de samenwerking, wat kan er volgende keer beter? De jaarlijkse evaluatie evolueert dan naar permanente evaluatie: dat stelt de auditcommissie in staat om geconstateerde verbeterpunten direct door te voeren.

IJkpunten voor de beoordeling

Bij de evaluatie van de auditcommissie kan het functioneren afgezet worden tegen:

- het reglement: zijn de daarin genoemde doelstellingen behaald? Zijn de taken en verantwoordelijkheden goed uitgevoerd? Voldoet de samenstelling nog aan de behoefte van de organisatie? Is er voldoende expertise aanwezig in de auditcommissie?;
- best practices: wat kan de auditcommissie leren en lenen van de werkwijze van andere

auditcommissies (bijvoorbeeld bij andere organisaties waar de voorzitter en de leden toezichtfuncties vervullen en/of in de auditcommissie zitting hebben)?;

- de eigen visie van de voorzitter en de leden: hoe kijken zij aan tegen het functioneren, de rolvulling en de onderlinge dynamiek? De visie van het bestuur en degene die verantwoordelijk is voor de duurzaamheidsverslaggeving in het bijzonder: hoe ervaren zij de auditcommissie? Worden er voldoende kritische vragen gesteld?;
- de visie van de externe accountant: welke observaties en inzichten zijn opgedaan bij de aanwezigheid tijdens de vergaderingen? Hoe verhoudt het functioneren zich tot dat van auditcommissies bij andere organisaties?

Ook Internal Audit en de bestuurssecretaris kunnen waardevolle inzichten in het functioneren van de auditcommissie verschaffen.

Evaluatie auditcommissie als team

Bij de evaluatie wordt allereerst het functioneren van de collectieve auditcommissie beoordeeld.

Daarbij kan gekeken worden naar:

- samenstelling van de commissie: achtergrond, expertise en rollen;
- opleiding en hulpmiddelen;
- eigen informatievergaring;
- verloop vergaderingen;
- kritische opstelling;
- onderlinge verhoudingen/samenwerking;
- relatie met het bestuur/management;
- relatie met interne en externe accountant;

- opvolging attentiepunten uit de vorige zelfevaluatie.

Evaluatie individuele leden

De voorzitter van de auditcommissie of de raad van commissarissen kan het functioneren van ieder lid van de auditcommissie beoordelen. Als de evaluatie extern begeleid wordt, kan aan de leden van de auditcommissie gevraagd worden om een peerreview: een beoordeling van het functioneren van de collega's in de commissie. Daarbij kan aandacht worden besteed aan:

- bedrijfskennis;
- expertisegebieden;
- objectiviteit en onafhankelijkheid;
- inzicht in de taken en verantwoordelijkheden van de commissie;
- bereidheid om tijd te besteden aan de voorbereiding van vergaderingen;
- aanwezigheid tijdens vergaderingen;
- rolinvulling en samenwerking.

Ook de lijst met competenties voor leden van de auditcommissie kan gebruikt worden voor evaluatie.

Evaluatie van de voorzitter

Het functioneren van de voorzitter van de auditcommissie wordt apart geëvalueerd, bijvoorbeeld door de voorzitter van de raad van commissarissen. De voorzitter van de auditcommissie zal bijvoorbeeld beoordeeld worden op zijn of haar vermogen om relaties te onderhouden met alle belangrijke spelers, de vergaderingen te leiden en de samenwerking in de commissie te optimaliseren. Ook voor de evaluatie

van de voorzitter kan gebruikgemaakt worden van de eerdergenoemde lijst met competenties.

Na de evaluatie

Een evaluatie heeft weinig nut zonder het formuleren van een plan van aanpak om aan de verbeterpunten te werken. De voorzitter van de auditcommissie moet de opvolging daarvan monitoren. De uitkomsten van de evaluatie van de auditcommissie worden met de raad van commissarissen besproken. Deze vermeldt in het externe verslag hoe de evaluatie van de auditcommissie (naast die van de raad van commissarissen zelf en de overige commissies) heeft plaatsgevonden en wat is of wordt gedaan met de conclusies van de evaluatie.

Best practices voor de evaluatie

- Heb oog voor de waarde van een robuust (zelf)evaluatieproces voor de commissie: het bevorderen van de dialoog, goede onderlinge verhoudingen en excellente prestaties.
- Beoordeel of het bestaande evaluatiebeleid effectief is en zorg dat de commissie de uitkomsten bespreekt.
- Monitor of de commissie geconstateerde verbeterpunten daadwerkelijk heeft doorgevoerd.



Bijlagen

Bijlage 1A	Vrijstellingen voor de verplichte instelling van een auditcommissie
Bijlage 1B	Suggesties voor het reglement van de auditcommissie
Bijlage 1C	Criteria voor de (non-)financiële deskundigheid van de auditcommissieleden
Bijlage 1D	Achtergrondinformatie voor nieuwe auditcommissieleden
Bijlage 1E	Voorbeeldplanner vergaderagenda auditcommissie
Bijlage 1F	Wie woont de vergadering van de auditcommissie bij?

Bijlage 1A Vrijstellingen voor de verplichte instelling van een auditcommissie

1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Vrijstellingen

Het Besluit instelling auditcommissie voorziet (via artikel 3) in vier vrijstellingen voor de verplichting tot het instellen van een auditcommissie. Het betreft vrijstellingsopties voor:

- a. een dochtermaatschappij als bedoeld in artikel 2:24a, eerste lid, van het Burgerlijk Wetboek van een rechtspersoon die voldoet aan artikel 39, leden 1, 2 en 5, van de richtlijn (2014/56/EU) en artikel 11, leden 1 en 2, en artikel 16, lid 5, van de EU-verordening (nr. 537/2014);
- b. een bank waarop een vrijstelling als bedoeld in artikel 3:111, eerste lid, van de Wet op het financieel toezicht van toepassing is indien een centrale kredietinstelling de in artikel 2, tweede lid, genoemde taken heeft opgedragen aan een auditcommissie waarvan de samenstelling voldoet aan artikel 2, eerste en derde lid (van het besluit);
- c. een beleggingsinstelling of icbe als bedoeld in artikel 1:1 van de Wet op het financieel toezicht die is opgenomen in het register als bedoeld in artikel 1:107 van de Wet op het financieel toezicht;
- d. een entiteit voor securitisatiedoeleinden als bedoeld in artikel 1 van het Besluit prudentiële regels Wft, mits de onderneming aan het publiek bekendmaakt waarom zij het niet dienstig acht een auditcommissie in te stellen, of een orgaan aan te wijzen in de zin van artikel 2, vierde lid (van het besluit).

Een in Nederland regelmatig toegepaste vrijstelling heeft betrekking op de dochtermaatschappij waarbij de moeder van de groep ook een auditcommissie heeft die aan de Europese vereisten voor een auditcommissie voldoet.

De nota van toelichting op de wetswijziging bevat nadere duiding over de bedoeling en toepassing van deze specifieke vrijstellingsoptie, die mede afhankelijk is van in welke EU-lidstaat de moeder is gevestigd. De bestuurders van een OOB die gebruikmaakt van deze ‘moeder-dochter’-vrijstellingsoptie doen er verstandig aan een bevestiging op te vragen van het bestuur van de moederverenootschap dat de auditcommissie voldoet aan de vereisten die in het Besluit-AC zijn genoemd. Op die manier kan worden onderbouwd dat op juiste gronden gebruik wordt gemaakt van de vrijstelling.



1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Vrijstelling voor het instellen van een auditcommissie als de moeder van de groep al een auditcommissie heeft ingesteld die aan specifieke voorwaarden voldoet

Het Besluit-AC is niet van toepassing op een dochtermaatschappij als bedoeld in artikel 2:24a, eerste lid, van het Burgerlijk Wetboek van een rechtspersoon die voldoet aan artikel 39, leden 1, 2 en 5, van de richtlijn en artikel 11, leden 1 en 2, en artikel 16, lid 5, van de EU-Auditverordening. Kort samengevat moet de auditcommissie van de moederverenootschap van de OOB voldoen aan de volgende vereisten:

- De auditcommissie is een autonome commissie of een commissie van het leidinggevend of toezichthoudend orgaan van de gecontroleerde entiteit. De auditcommissie is samengesteld uit niet bij het dagelijks bestuur betrokken leden van het leidinggevende orgaan en/of leden van het toezichthoudende orgaan van de gecontroleerde entiteit en/of leden die worden benoemd door de algemene aandeelhoudersvergadering van de gecontroleerde entiteit of, voor entiteiten zonder aandeelhouders, door een soortgelijk orgaan.
- Ten minste één lid van de auditcommissie beschikt over de nodige deskundigheid op het gebied van financiële verslaglegging en/of controle van financiële overzichten.
- De leden van de commissie als geheel beschikken over deskundigheid die relevant is voor de sector waarin de gecontroleerde entiteit actief is.

- De meerderheid van de leden van de auditcommissie is onafhankelijk van de gecontroleerde entiteit. De voorzitter van de auditcommissie wordt benoemd door de leden van het commissie of door het toezichthoudende orgaan van de gecontroleerde entiteit, en is onafhankelijk van de gecontroleerde entiteit. De lidstaten kunnen eisen dat de voorzitter van de auditcommissie jaarlijks wordt gekozen door de algemene aandeelhoudersvergadering van de gecontroleerde entiteit.
- Wettelijke accountants of accountantskantoren die wettelijke controles van financiële overzichten van OOB's uitvoeren, dienen een aanvullende verklaring in bij de auditcommissie van de gecontroleerde entiteit niet later dan de indiening van de controleverklaring bij de jaarrekening. Deze aanvullende verklaring aan de auditcommissie is op schrift gesteld. Zij licht de resultaten van de uitgevoerde wettelijke controle toe en bevat ten minste de in artikel 11 lid 2 van de EU-Auditverordening genoemde elementen.
- Het voorstel aan de algemene aandeelhouders- of ledenvergadering van de gecontroleerde entiteit voor de benoeming van wettelijke accountants of accountantskantoren omvat de in artikel 16 lid 2 van de EU-Auditverordening bedoelde aanbeveling en voorkeur van de auditcommissie. In het voorstel wordt vermeld waarom de aanbeveling van de auditcommissie of het orgaan dat soortgelijke functies uitoefent is opgevolgd. Als het voorstel afwijkt van de

voorkeur van de auditcommissie, wordt in het voorstel vermeld waarom de aanbeveling van de auditcommissie niet is gevolgd.



Bijlage 1B Suggesties voor het reglement van de auditcommissie

1. Commissie

1. Het reglement

2. Samenstelling van de auditcommissie

3. De rol van de voorzitter

4. Vergaderingen

5. Evaluatie van de auditcommissie

Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

1. Doelstellingen De auditcommissie is een vaste commissie van de raad van commissarissen. De auditcommissie ondersteunt de raad van commissarissen bij het uitvoeren van de verantwoordelijkheden op het terrein van toezicht op: 1.1 de werking van de interne risicobeheersings- en controlesystemen, waaronder het toezicht op de naleving van de relevante wet- en regelgeving en het toezicht op de werking van gedragscodes; 1.2 de financiële en niet-financiële informatie-verschaffing door de organisatie (keuze van verslaggevings- grondslagen, toepassing en beoordeling van effecten van nieuwe regels, inzicht in de behandeling van ‘schattingsposten’ in de jaarrekening, prognoses, werk van Internal Audit en de externe accountant terzake, et cetera.); 1.3 de naleving van aanbevelingen en opvolging van opmerkingen van Internal Audit en de externe accountant; 1.4 de relatie met, de rol en het functioneren van Internal Audit; 1.5 het belastingbeleid van de organisatie; 1.6 de relatie met de externe accountant; 1.7 het formeel jaarlijks evalueren van de onafhankelijkheid van de externe accountant en	de kwaliteit van de controledienstverlening; 1.8 voorafgaande goedkeuring van controlediensten, aan de controle gerelateerde werkzaamheden en toegestane niet-controlediensten geleverd door de externe accountant om de onafhankelijkheid van de externe accountant te bewaken; 1.9 de financiering van de organisatie; 1.10 de toepassingen van de informatie- en communicatietechnologie (ICT) waaronder risico’s op het gebied van cybersecurity en privacy; 1.11 de voordracht tot (her)benoeming van een externe accountant door de algemene vergadering; 1.12 het uitbrengen van advies inzake de jaarrekening en de jaarlijkse begroting en belangrijke investeringen aan de raad van commissarissen. Bij het uitvoeren van haar taken onderhoudt de commissie een effectieve werkrelatie met de raad van commissarissen, het management, Internal Audit en de externe accountant. Om zijn of haar rol effectief te vervullen, verkrijgt ieder commissielid inzicht, op detailniveau, in de verantwoordelijkheden die aan het lidmaatschap van de commissie zijn verbonden, alsmede in de organisatie, haar activiteiten en de risico’s waaraan de organisatie blootstaat
--	---

2. Bevoegdheid De raad van commissarissen machtigt de auditcommissie om binnen de reikwijdte van haar verantwoordelijkheden: 2.1 elke vorm van informatie die zij nodig heeft, in te winnen bij: elke werknemer (en alle werknemers worden geïnstrueerd mee te werken aan elk verzoek van de auditcommissie), en externe partijen; 2.2 extern juridisch of ander professioneel advies in te winnen; 2.3 ervoor te zorgen dat, indien daaraan behoefte bestaat, functionarissen van de organisatieen bij vergaderingen aanwezig zijn. 3. Organisatie Lidmaatschap 3.1 de commissie bestaat uit ten minste drie leden. 3.2 ieder lid moet in staat zijn een waardevolle bijdrage aan de commissie te leveren. 3.3 maximaal één lid hoeft niet onafhankelijk zijn. Dit lid kan echter geen voorzitter van de commissie zijn. 3.4 de voorzitter van de auditcommissie wordt periodiek door de raad van commissarissen voorgedragen.	3.5 het voorzitterschap wordt niet vervuld door de voorzitter van de raad van commissarissen, noch door een voormalig bestuurder van de organisatie. 3.6 leden worden benoemd voor een periode van [aantal] jaar. 3.7 voor elke vergadering geldt een quorum van [aantal] leden. 3.8 de secretaris van de auditcommissie is de secretaris van de organisatie, of een andere door de raad van commissarissen benoemde persoon. 3.9 de auditcommissie stelt vast dat de organisatie in haar jaarverslag de samenstelling van de auditcommissie vermeldt. 3.10 ten minste één lid van de auditcommissie moet een financieel expert zijn, hetgeen inhoudt dat deze persoon relevante kennis en ervaring heeft opgedaan op financieel-administratief/ accountingterrein bij een beursgenoteerde organisatie of bij andere grote rechtspersonen. Bijwonen van vergaderingen 3.11 de auditcommissie mag iedere persoon (bijvoorbeeld de president-directeur (ceo), de financieel directeur (cfo), het hoofd Internal Audit) uitnodigen van wie men de aanwezigheid tijdens de vergaderingen noodzakelijk acht. De auditcommissie bepaalt dit zelf.
---	--

- 1. Commissie**
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
 - 4. Vergaderingen
 - 5. Evaluatie van de auditcommissie**Bijlagen**
- 2. Continuïteit**
- 3. Corporate impact**
- 4. Control & Compliance**
- 5. Cultuur en gedrag**
- 6. Checks & Balances**
- 7. Corporate Reporting**
- 8. Crisis**
- 9. Communicatie**

3.12 Internal audit en de externe accountant moeten in voorkomende gevallen worden uitgenodigd presentaties voor de auditcommissie te houden. De externe accountant woont in ieder geval de vergadering bij waarin wordt gesproken over zijn verslag met betrekking tot het onderzoek van de jaarrekening.

3.13 de auditcommissie overlegt zo vaak als zij dit nodig acht, maar minstens eenmaal per jaar buiten aanwezigheid van de leden van de raad van bestuur met de externe accountant.

3.14 vergaderingen worden ten minste driemaal per jaar gehouden (minimaal voor de bepaling van de scope van werkzaamheden, de bespreking van de jaarrekening en voor de bespreking van de halfjaarcijfers). Bijzondere vergaderingen kunnen bijeengeroepen worden zodra hieraan behoefte bestaat. Internal Audit of de externe accountant mag een vergadering bijeenroepen indien dit noodzakelijk wordt geacht.

3.15 de handelingen van alle vergaderingen worden genotuleerd.

3.16 de commissie stelt vast dat de organisatie in haar jaarverslag het aantal vergaderingen van de auditcommissie en de belangrijkste onderwerpen die aan de orde zijn gekomen vermeldt.

3.17 de raad van commissarissen ontvangt van de auditcommissie een verslag van de beraadslagingen en bevindingen.

4. Rollen en verantwoordelijkheden van de auditcommissie

Interne risicobeheersings- en controlesystemen
4.1 beoordeelt of het management de juiste ‘beheersingscultuur’ uitdraagt door het belang van interne beheersing en risicomanagement te communiceren en of het management ervoor zorgt dat alle werknemers inzicht hebben in hun rollen en verantwoordelijkheden.

4.2 verkrijgt inzicht in de mate waarin aanbevelingen van Internal Audit en de externe accountant met betrekking tot de interne beheersing door het bestuur zijn geïmplementeerd.

Informatie- en communicatietechnologie
4.3 beoordeelt de toepassing van informatie- en communicatietechnologie door de organisatie, waaronder risico’s op het gebied van cybersecurity en beoordeelt op welke wijze het management zich verantwoordt over de (cyber) beveiliging van computersystemen en applicaties, en de calamiteitenplanning ten aanzien van de verwerking van (financiële en andere) gegevens in het geval zich ernstige systeemstoringen, cyberaanvallen, datalekken of inbreuk op privacy voordoen.

Belastingbeleid
4.4 richt zich op het toezicht op het bestuur ten aanzien van het belastingbeleid van de organisatie.

Financiële informatieverschaffing

Algemeen
4.5 verkrijgt inzicht in de gebieden waarop momenteel de grootste financiële risico’s worden gelopen en in de wijze waarop het management deze risico’s effectief beheerst.

4.6 beoordeelt samen met Internal Audit en de externe accountant eventuele fraude, illegale handelingen, tekortkomingen in de interne beheersing of andere soortgelijke zaken.

4.7 beoordeelt belangrijke kwesties op het gebied van verslaggeving, met inbegrip van recente uitspraken van regelgevende en beroepsorganisaties, en begrijpt de invloed hiervan op de jaarrekening.

4.8 informeert bij het management, Internal Audit en de externe accountant naar de belangrijke risico’s en uitstaande posities, en de plannen om dergelijke risico’s te minimaliseren.

4.9 beoordeelt eventuele juridische zaken die de jaarrekening in belangrijke mate zouden kunnen beïnvloeden.

Jaarrekening
4.10 beoordeelt de jaarrekening en stelt vast dat deze volledig is en in overeenstemming met de informatie die bij de commissieleden bekend is.

Beoordeelt of de jaarrekening is gebaseerd op de juiste grondslagen voor financiële verslaggeving.

4.11 schenkt bijzondere aandacht aan complexe en/of ongebruikelijke transacties zoals herstructureringskosten en verslaggeving van derivaten.

4.12 richt zich op gebieden waarbij oordeelsvorming een belangrijke rol speelt, bijvoorbeeld met betrekking tot de waardering van activa en passiva, garantie, product- of milieuaansprakelijkheid, voorzieningen in verband met gerechtelijke procedures en overige (niet uit de balans blijvende) verplichtingen.

4.13 bespreekt de jaarrekening en de uitkomsten van de jaarrekeningcontrole met het management en de externe accountant.

4.14 beoordeelt, voorafgaand aan de bekendmaking, de overige onderdelen van het bestuursverslag en gaat na of de informatie begrijpelijk is en in overeenstemming met de kennis die de leden over de organisatie en haar activiteiten hebben.

Voorlopige aankondigingen, tussentijdse cijfers en informatieverstrekking aan analisten
4.15 laat zich inlichten over de wijze waarop de leiding voorlopige aankondigingen, tussentijdse cijfers en informatie ten behoeve van analisten tot stand brengt; over de betrokkenheid van de Internal Audit; en over de mate waarin de externe accountant dergelijke informatie beoordeelt.

1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

4.16 beoordeelt de getrouwheid van de voorlopige en tussentijdse cijfers en toelichting, en verkrijgt een toelichting van het management, Internal Audit en de externe accountant over de mate waarin:

- de tussentijdse financiële resultaten belangrijk afwijken van de gebudgetteerde of geprognosticeerde resultaten;
- wijzigingen van financiële ratio's en verbanden in de tussentijdse cijfers consistent zijn met wijzigingen in de activiteiten en financieringswijze van de organisatie;
- algemeen aanvaarde grondslagen voor financiële verslaggeving bestendig zijn toegepast;
- er sprake is van daadwerkelijke of voorgestelde wijzigingen in de wijze van administratieve verwerking of externe verslaggeving van posten;
- er sprake is van belangrijke of ongebruikelijke gebeurtenissen of transacties;
- de financiële en operationele beheersingsmaatregelen van de organisatie effectief functioneren;
- de voorlopige aankondigingen en tussentijdse cijfers toereikende en relevante informatie bevatten.

Internal Audit

4.17 beoordeelt de activiteiten en de organisatiestructuur van Internal Audit en zorgt ervoor dat geen onterechte restricties worden aangebracht.

4.18 beoordeelt de kwalificaties van de medewerkers van Internal Audit en is mede verantwoordelijk voor de benoeming, vervanging, overplaatsing of het ontslag van het hoofd Internal Audit.

4.19 beoordeelt de effectiviteit van Internal Audit.

4.20 bespreekt afzonderlijk met het hoofd Internal Audit eventuele zaken waarvan de commissie of de accountant van mening is dat deze in beslotenheid moeten worden besproken.

4.21 richt zich op de relatie van het bestuur met de interne auditor en de naleving van aanbevelingen en opvolging van opmerkingen van Internal Audit door het bestuur.

4.22 zorgt ervoor dat het management reageert op aanbevelingen van Internal Audit.

Externe accountantscontrole

4.23 beoordeelt de door de externe accountant voorgestelde reikwijdte en aanpak van de controle en zorgt ervoor dat met betrekking tot de reikwijdte geen onterechte restricties of beperkingen zijn opgelegd.

4.24 beoordeelt het functioneren van de externe accountant.

- De auditcommissie rapporteert jaarlijks aan de raad van commissarissen over de ontwikkelingen in de relatie met de externe accountant, waaronder in het bijzonder zijn onafhankelijkheid (met inbegrip van de wenselijkheid van rotatie

van verantwoordelijke partners binnen een kantoor van externe accountants dat met de controle is belast en van het verrichten van niet-controlewerkzaamheden).

- De auditcommissie beoordeelt eens in de vier jaar grondig het functioneren van de externe accountant in de diverse entiteiten en capaciteiten waarin de externe accountant fungeert. De belangrijkste conclusies hiervan worden aan de algemene vergadering van aandeelhouders medegedeeld ten behoeve van de beoordeling van de voordracht tot benoeming van de externe accountant.
- De auditcommissie evalueert jaarlijks de onafhankelijkheid van de externe accountant, de kwaliteit van de controlediensten en een onderbouwing van het jaarlijkse controlebudget in verhouding tot het aanwezige controlerisico. Hierbij rapporteert de auditcommissie veranderingen in het beleid of de situatie in vergelijking met het vorige jaar.
- Gaat de onafhankelijkheid van de externe accountant na, hetgeen ook inhoudt dat de omvang van de verleende diensten wordt afgezet tegen alle adviesdiensten die door de organisatie worden afgenomen.

4.25 doet aanbevelingen aan de raad van commissarissen met betrekking tot de herbenoeming van de externe accountant.

4.26 bespreekt afzonderlijk met de externe accountant eventuele zaken waarvan de commissie of de accountant van mening is dat deze in beslotenheid moeten worden besproken.

4.27 stelt vast dat belangrijke bevindingen en aanbevelingen van de externe accountant tijdig worden ontvangen en besproken.

4.28 richt zich op de relatie van het bestuur met de externe accountant en de naleving van aanbevelingen en opvolging van opmerkingen van de externe accountant door het bestuur.

4.29 is het eerste aanspreekpunt voor de externe accountant, wanneer deze onregelmatigheden constateert in de inhoud van de financiële berichten.

4.30 beoordeelt de effectiviteit van het systeem voor de naleving van wet- en regelgeving, en de resultaten van onderzoek door het management naar frauduleuze handelingen of niet-naleving, en de vervolgstappen die worden genomen (waaronder disciplinaire maatregelen).

4.31 wordt regelmatig door het management en de bedrijfsjurist op de hoogte gesteld van de gang van zaken met betrekking tot de naleving van wet- en regelgeving.

4.32 vergewist zich ervan dat bij het opstellen van de jaarrekening rekening is gehouden met alle voorschriften.

4.33 beoordeelt de bevindingen naar aanleiding van eventuele onderzoeken door regelgevende en/of toezichthoudende instanties.

- 1. **Commissie**
 - 1. Het reglement
 - 2. Samenstelling van de auditcommissie
 - 3. De rol van de voorzitter
 - 4. Vergaderingen
 - 5. Evaluatie van de auditcommissie**Bijlagen**
- 2. **Continuïteit**
- 3. **Corporate impact**
- 4. **Control & Compliance**
- 5. **Cultuur en gedrag**
- 6. **Checks & Balances**
- 7. **Corporate Reporting**
- 8. **Crisis**
- 9. **Communicatie**

Naleving van de gedragscode van de organisatie (indien van toepassing)

4.34 zorgt ervoor dat de gedragscode schriftelijk is vastgelegd en dat maatregelen worden getroffen opdat alle medewerkers van de gedragscode op de hoogte zijn.

4.35 evalueert of het topmanagement de juiste ‘toon’ zet door het belang van de gedragscode en de richtlijnen voor aanvaardbaar gedrag te communiceren.

4.36 beoordeelt het proces waarmee de naleving van de gedragscode wordt bewaakt.

4.37 wordt regelmatig door het management geïnformeerd over nalevingskwesies en over reputatiemanagement.

Rapporteringseisen

4.38 stelt regelmatig de raad van commissarissen op de hoogte van commissieactiviteiten en doet relevante aanbevelingen. In het verslag wordt in ieder geval vermeld:

- i. de wijze waarop de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen is beoordeeld;
- ii. de wijze waarop de effectiviteit van het interne en externe controleproces is beoordeeld;
- iii. materiële overwegingen inzake de (non-) financiële verslaggeving; en
- iv. de wijze waarop de materiële risico's en onzekerheden zijn geanalyseerd en besproken en wat de belangrijkste bevindingen van de auditcommissie zijn.

4.39 zorgt ervoor dat de raad van commissarissen zich bewust is van zaken die een belangrijke invloed kunnen hebben op de financiële positie of activiteiten van de organisatie.

Overige verantwoordelijkheden

4.40 voert op verzoek van de volledige raad van commissarissen andere toezichthoudende activiteiten uit.

4.41 initieert, indien noodzakelijk, bijzondere onderzoeken en huurt, indien relevant, ter ondersteuning speciale adviseurs of experts in.

4.42 beoordeelt en actualiseert het reglement; legt wijzigingen ter goedkeuring voor aan de raad van commissarissen.

4.43 evalueert regelmatig het eigen functioneren van de commissie.

Onderzoeken in het kader van verplichtingen, investeringen en overnames.

4.46 beoordeelt de risico's en aandachtspunten die samenhangen met verplichtingen investeringen en overnames.



Bijlage 1C Criteria voor de (non-)financiële deskundigheid van de auditcommissieleden

1. Commissie

1. Het reglement
 2. Samenstelling van de auditcommissie
 3. De rol van de voorzitter
 4. Vergaderingen
 5. Evaluatie van de auditcommissie
- Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Wat kunnen we onder 'relevante financiële deskundigheid' verstaan?

In het algemeen:

- het probleemloos kunnen analyseren van (non-)financiële rapportages;
- weten welke vragen gesteld moeten worden en hoe de antwoorden moeten worden geïnterpreteerd;
- bereid zijn om de (non-)financiële deskundigheid op niveau te houden;
- genoeg weten om leden en de organisatie uit de problemen te houden;
- een breed inzicht hebben in de van toepassing zijnde accounting principles (bijvoorbeeld IFRS) en de verslaggevingsregels rondom duurzaamheid (bijvoorbeeld CSRD);
- begrijpen wat de (non-)financiële zaken zijn die aan de auditcommissie worden uitgelegd;
- het vertrouwen hebben om aanvullende vragen te stellen tot u tevreden bent;
- herkennen wanneer (non-)financiële rapportages niet 'goed' voelen;
- begrijpen hoe interne controles en procedures met het oog op de (non-)financiële rapportage werken;
- ook het perspectief van investeerders en andere externe stakeholders kunnen hanteren.

In individuele gevallen:

- begrijpen hoe de jaarrekening wordt samengesteld;
- begrip hebben van de subjectieve onderwerpen en van onderwerpen waar een oordeel over moet worden geveld;
- begrijpen op welke alternatieve wijze de (non-)financiële verslaggevingsstandaarden hadden kunnen worden toegepast;
- de basale tests begrijpen om de kwaliteit van de inkomsten en de financiële positie te toetsen, bijvoorbeeld het vergelijken van de inkomsten met de kasstromen.

Om tot de benodigde (non-)financiële deskundigheid te komen kan het voldoende zijn om in auditcommissies zitting te hebben. Als een persoon echter maar van één auditcommissie lid is, loopt hij of zij het gevaar dat de deskundigheid statisch wordt. Dan is het met name belangrijk om door middel van updates en trainingen de vaardigheden op niveau te houden. Trainingen en updates zijn echter niet zo belangrijk als het vermogen van een persoon om de juiste vragen te stellen, vasthoudend te zijn en waar nodig uit te dagen.



Bijlage 1D Achtergrondinformatie voor nieuwe commissieleden

1. Commissie

1. Het reglement

2. Samenstelling van de auditcommissie

3. De rol van de voorzitter

4. Vergaderingen

5. Evaluatie van de auditcommissie

Bijlagen

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Nieuwe leden van de auditcommissie hebben achtergrondinformatie nodig over vele onderwerpen, onder andere over:

De organisatie

- producten en diensten;
- belangrijke risicogebieden en de manier waarop deze worden beheerst;
- beschrijving van het stelsel van risicomanagement en interne beheersing voor zowel de strategische, operationele, financiële, niet-financiële, compliance- en verslaggevingsrisico's;
- belangrijke grondslagen van waardering en resultaatbepaling en waarom zij worden gebruikt;
- belangrijke aandachtsgebieden met betrekking tot de financiële positie en de gerapporteerde waarde van de individuele activa en passiva;
- wettelijke verslaggevings- en beursnoteringsvereisten waaraan de organisatie moet voldoen, inclusief verslaggeving rondom duurzaamheid;
- buitenlandse en binnenlandse activiteiten;
- betrokkenheid van de organisatie bij gerechtelijke procedures of onvoorziene posten;
- onzekerheden waar de organisatie mee te maken heeft;
- ontwikkeling van de financiële positie (tussentijdse en jaarcijfers);
- de gedragscode van de organisatie en het gedrag in de praktijk en de rol van de auditcommissie bij het toezicht op het management inzake de bewaking van de naleving van deze code;
- het belastingbeleid.

Management

- de achtergrond en kwalificaties van het financieel en topmanagement;
- een organogram waaruit de rapportagelijnen en -verantwoordelijkheden blijken;
- de basis van de beloning voor het senior management.

De auditcommissie

- het reglement van de auditcommissie – haar rol in het toezicht op het beleid van de organisatie, de financiële verslaggeving en andere specifieke gebieden;
- de medewerkers die ter ondersteuning van de auditcommissie beschikbaar zijn;
- externe adviseurs die ter ondersteuning van de auditcommissie beschikbaar zijn;
- de aard en timing van rapporten opgesteld door het management voor de commissie.

Interne auditor

- de verantwoordelijkheden van Internal Audit;
- het aantal interne auditors en hun kwalificaties en ervaring;
- de relatie van de commissie met Internal Audit;
- het soort informatie dat de auditcommissie van Internal Audit ontvangt;
- het auditplan van Internal Audit voor het onderhavige jaar;
- resultaten van onafhankelijke beoordelingen van Internal Audit;
- recente rapportages van Internal Audit.

Externe accountant

- een kopie van de opdrachtbevestiging voor de externe controle voor het onderhavige jaar;
- de reikwijdte van de externe accountantscontrole, inclusief het controleplan voor het onderhavige jaar.
- de relatie van de commissie met de externe accountant;
- het soort informatie dat de auditcommissie van de externe accountant ontvangt;
- de verschillende soorten rapporten die de externe accountant uitbrengt en wanneer deze worden uitgebracht;
- recente rapportages van de externe accountant;
- het beleid van de organisatie met betrekking tot het geven van controle en niet-controleopdrachten aan de accountant.



Bijlage 1E Voorbeeldplanner vergaderagenda auditcommissie

1. Commissie
1. Het reglement
2. Samenstelling van de auditcommissie
3. De rol van de voorzitter
4. Vergaderingen
5. Evaluatie van de auditcommissie
- Bijlagen
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis
9. Communicatie

Agenda onderwerp	Januari/ februari	April/ mei	Juni/ juli	September/ oktober	November/ december
Interne en externe verslaggeving					
Planning-en-controlcyclus: financiële meerjarenprojecties, uitgangspunten (meerjaren)begroting, jaarbegroting, periodieke managementinformatie	■	■	■	■	■
Belangrijke schattingen en aannames (materiële overwegingen in de financiële verslaggeving)	■				
Nieuwe verslaggevingsstandaarden: impact en (voortgang) implementatieplan			■		
Kwartaalrapportage (indien van toepassing)		■	■	■	
(Concept)jaarrekening	■				■
(Concept)bestuursverslag / Integrated Report	■				■
Bestuursverklaring in het bestuursverslag (onderbouwing)	■				
Juridische claims en geschillen	■	■	■	■	■
Transacties met verbonden partijen	■		■		
Evaluatie van de financiële functie (inclusief competentiereview en opvolgingsplanning)			■		
Financiering					
Treasuryplan en -ontwikkelingen		■			■
Risicomanagement en Compliance					
Risicobeheersing: evaluatie door het bestuur van:					
- Ontwikkeling risicoprofiel					
- Effectieve opzet en werking van het stelsel van risicobeheersing		■			■
- Tekortkomingen, bijsturing en geplande verbeteringen					
- Risicobereidheid					
ICT inclusief cybersecurity		■	■		■
- ICT-ontwikkelingen en ICT-risicobeheersing					
- Belangrijkste systeemwijzigingen en implementatie nieuwe systemen					
- Cybersecurityrisico's					
- Digitaliseringsagenda					
Frauderisicoanalyse				■	
Verzekeringsbeleid (update)			■		
Cultuur en gedrag:					
- Evaluatie naleving gedragscode	■	■	■	■	■
- Compliance- en businessconductrapportages (inclusief meldingen van klokkenluiders en schendingen)					
Belastingbeleid					
Belastingbeleid (wijzigingen)				■	
Tax-compliance	■				

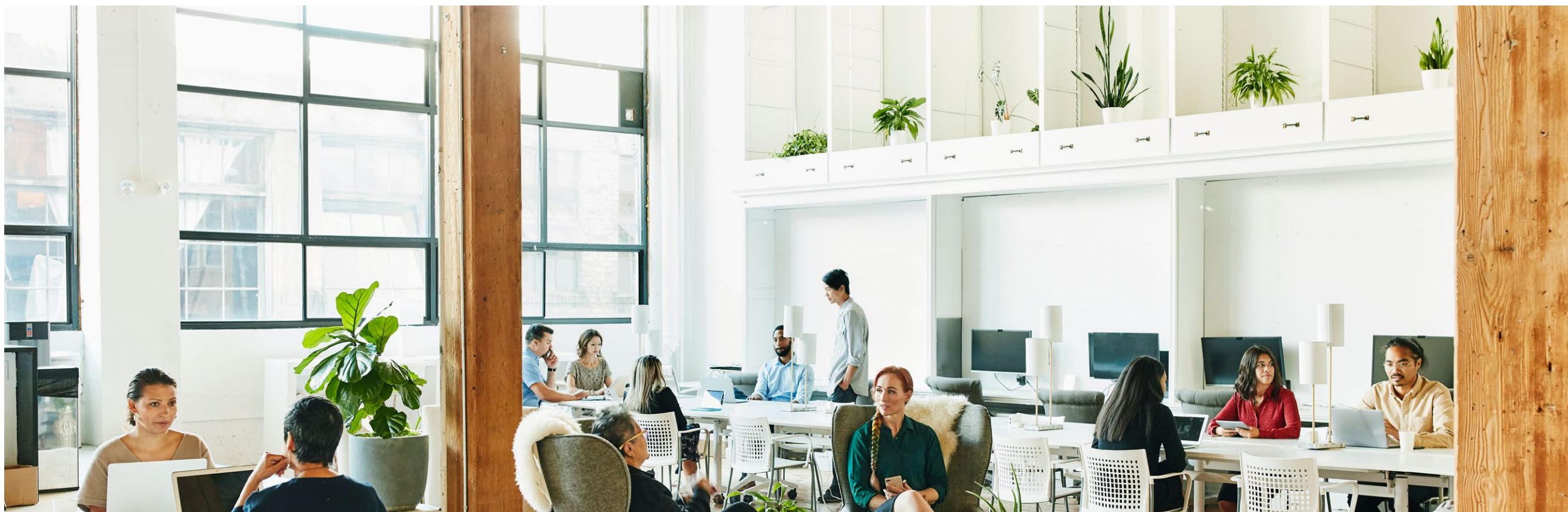
1. Commissie
1. Het reglement
2. Samenstelling van de auditcommissie
3. De rol van de voorzitter
4. Vergaderingen
5. Evaluatie van de auditcommissie
- Bijlagen
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis
9. Communicatie

Agendaonderwerp	Januari/ Februari	April/ Mei	Juni/ Juli	September/ Oktober	November/ December
Internal audit					
Internal Audit-jaarplan (vaststellen)	■				
Internal Audit-activiteitenverslag en update van het jaarplan			■		
Internal Audit-onderzoeksresultaten (rapportages): beoordeling interne beheersing	■	■	■	■	■
Opvolging aanbevelingen Internal Audit en externe accountant	■	■	■	■	■
Beoordeling van het Internal Audit reglement					■
Jaarlijkse evaluatie Internal Audit (inclusief formatie, competentiereview, opvolgingsplanning en eventuele samenwerkingsovereenkomsten)					■
Externe accountant					
Controleplan en -honorarium		■			
Voorafgaande goedkeuring (pre-approval) diensten externe accountant (en honoraria)	■	■	■	■	■
Rapportage interim-bevindingen				■	
Accountantsverslag en controleverklaring	■				
Evaluatie van het functioneren van en ontwikkelingen in de relatie met de externe accountant	■				
Beoordeling onafhankelijkheid van de accountant	■				
(Her)benoeming van de externe accountant	■				
Algemeen					
Besloten deel van de vergadering (executive session)	■	■	■	■	■
Vaststellen notulen auditcommissie vergadering	■	■	■	■	■
Vaststelllen van het auditcommissie-jaarplan					■
Jaarlijkse zelfevaluatie auditcommissie	■				
Beoordeling van het auditcommissiereglement					■
Verslag auditcommissie aan de raad van commissarissen (zoals bedoeld in Code best practice bepaling 1.5.3)	■				
Verslag raad van commissarissen in het jaarverslag (in bijzonder sectie over auditcommissie)	■				
Besloten sessies ('private sessions')					
Elke vergadering: cfo, Internal Audit, externe accountant	■	■	■	■	■
Op verzoek van de auditcommissie, bijvoorbeeld CISO, cio, director Tax, Legal Counsel					
Specifieke onderwerpen en 'deep dives'					
Organisatiespecifiek in te vullen onderwerpen	■	■	■	■	■

Bijlage 1F Wie woont de vergadering van de auditcommissie bij?

1. Commissie
1. Het reglement
2. Samenstelling van de auditcommissie
3. De rol van de voorzitter
4. Vergaderingen
5. Evaluatie van de auditcommissie
- Bijlagen
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis
9. Communicatie

Persoon/team	Frequentie	Reden
Hoofd Internal Audit	Iedere vergadering	- Om voortgang te bespreken in auditjaarplan, de onderzoeksresultaten, de opvolging in de aanbevelingen en om overkoepelende thema's ten aanzien risico- en controlesystemen te bespreken - Om eventuele wijzigingen in het (lopende) auditjaarplan te bespreken - Om deel te nemen aan een discussie over belangrijke risico's - Om zaken te bespreken die de (non-)financiële verslaglegging kunnen beïnvloeden, zoals belangrijke schattingen en aannames - Om mogelijke override of internal controls of indicaties van mogelijk wangedrag van bestuur of senior management te bespreken
Externe accountant	Iedere vergadering	- Om deel te nemen aan een discussie over belangrijke risico's - Om zaken te bespreken die de financiële verslaglegging kunnen beïnvloeden, zoals belangrijke schattingen en aannames - Belangrijke interne controles
Belangrijke medewerkers: - cfo - Risicomanagement/ Compliance	Iedere vergadering	- Om deel te nemen aan een discussie over belangrijke risico's - Om zaken te bespreken die de financiële verslaglegging kunnen beïnvloeden, zoals belangrijke schattingen en aannames - Belangrijke interne controles
Belangrijke medewerkers: - De juridisch adviseur - Human Resources - Marketing/Sales - Lijnmanagement	Iedere vergadering	Risicomanagement/Compliance - Om het management van informatie te voorzien omtrent de belangrijkste bestaande en opkomende risico's - Om informatie te verschaffen over significante compliance-zaken, inclusief het beleid, processen en de cultuur - Om informatie te verschaffen over klachten, inclusief klokkenluiden
	Bij de meeste vergaderingen	Chief financial officer Om informatie te verschaffen over het (non-)financiële verslagleggingsproces, inclusief de belangrijkste (non-)financiële risico's, controles en financiële verslaggevingsstandaarden.
	Eén keer per jaar, of vaker als er zich juridische kwesties voordoen	De juridisch adviseur - Om te adviseren over eventuele juridische inbreuken of schendingen van de gedragscode van de organisatie. - Om alle belangrijke juridische risico's uit te leggen waarmee de organisatie wordt geconfronteerd en die de druk tot fraude kunnen doen toenemen.
	Jaarlijks	Human Resources Om informatie te verschaffen over de integriteit van het bestuur en over de toon aan de top
	Jaarlijks	Sales en Marketing Om informatie te verschaffen over het beleid en de controles op het gebied van verkoopactiviteiten. Deze informatie kan helpen om vast te stellen of er druk ontstaat om de omzettargets te behalen die mogelijk kan leiden tot ongepast gedrag.
	Twee keer per jaar	Lijnmanagement Om te bespreken of er prestatiebonussen zijn of druk wordt uitgeoefend door het bestuur die er mogelijk voor kunnen zorgen dat interne controles worden omzeild door het management.
Indien mogelijk organiseert de auditcommissie aparte vergaderingen met het (lijn)management, Internal Audit en de externe accountant. Onderwerpen die mogelijk met het management kunnen worden besproken, zijn de evaluatie van Internal Audit en de externe accountant en het accountingproces. De gesprekken met Internal Audit en de externe accountant kunnen gaan over de samenwerking die wordt ervaren met het personeel en het bestuur en senior management van de onderneming.		



Continuïteit

Duurzame langetermijnwaardecreatie

02

2. Continuïteit - duurzame langetermijnwaardecreatie

1. Commissie

2. Continuïteit

1. Toetsen strategische besluitvorming
2. Beoordelen strategie, business- en investeringsplannen
3. Monitoren van het waardecreatieproces
4. Signaleren van risico's

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Toezicht op continuïteit en duurzame langetermijnwaardecreatie vormt een van de pijlers van goed bestuur. De rol van de auditcommissie daarbij: een gedegen beoordeling van de levensvatbaarheid, financiering en risico's van het businessmodel en een zorgvuldige monitoring van het waardecreatieproces en de uitvoering van de strategie.

Continuïteit en duurzame langetermijnwaardecreatie vormen kernthema's in hedendaagse governance. De afgelopen jaren is er naast gerichtheid op de korte termijn winstmaximalisatie en aandeelhouderswaarde een toenemende focus ontstaan op het creëren van duurzame waarde voor een bredere groep stakeholders: niet alleen aandeelhouders en andere kapitaalverschaffers, maar ook bijvoorbeeld werknemers, klanten, leveranciers en de maatschappij in het algemeen. Daarbij is er sprake van een toenemende aandacht voor de maatschappelijke impact van organisaties. In dit hoofdstuk ligt de focus op duurzame langetermijnwaardecreatie in financiële zin en het waarborgen van de continuïteit in bedrijfsmatige zin. In hoofdstuk 3 (Corporate impact) komen stakeholderbelangen en maatschappelijke waardecreatie aan de orde.

Hernieuwd bewustzijn van brede taakstelling

De aandacht voor continuïteit en langetermijnwaardecreatie in het denken over goed bestuur en de Code heeft een grote invloed op de taken en verantwoordelijkheden van de raad van commissarissen en daarmee de auditcommissie. Eigenlijk is er sprake van een hernieuwd bewustzijn van de wettelijke brede taakstelling van de raad van commissarissen: deze houdt toezicht op het beleid van het bestuur en richt zich daarbij op de belangen van alle stakeholders.

Duurzaam handelen

De Code vult die verantwoordelijkheid nog iets explicieter in: van bestuurders en commissarissen wordt verwacht dat zij zich richten op duurzame langetermijnwaardecreatie. Bij de bepaling van de strategie staat 'de houdbaarheid en duurzaamheid op de lange termijn' centraal. De Code legt eveneens meer accent op continuïteit en op transparantie over de risico's en onzekerheden die deze op zowel de korte als de lange termijn kunnen bedreigen.



In dit hoofdstuk komen de volgende onderwerpen aan de orde:

1. Toetsen strategische besluitvorming
2. Beoordelen strategie, business- en investeringsplannen
3. Monitoren van het waardecreatieproces
4. Signaleren van risico's

Snelle veranderingen in concurrentieveld en keten

Continuïteit is uiteraard niet vanzelfsprekend. Organisaties worden in toenemende mate geconfronteerd met risico's en onzekerheden door snelle veranderingen in de maatschappij, het concurrentieveld en de keten (zie de vijf megatrends op de volgende pagina).

De levensduur van bedrijven die zich niet weten aan te passen neemt steeds verder af. Dat vraagt om continu anticiperen op externe ontwikkelingen, de vertaling daarvan in nieuwe businessmodellen en bovenal strategische wendbaarheid om bedreigingen voor te zijn en kansen te grijpen.

1. Commissie

2. Continuïteit

- 1. Toetsen strategische besluitvorming
- 2. Beoordelen strategie, business- en investeringsplannen
- 3. Monitoren van het waardecreatieproces
- 4. Signaleren van risico's

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

De gevolgen van de megatrends: ADAPT



	Assymetry	Disruption	Age	Polarisation	Trust
Bedreiging	De kloof tussen arm en rijk wordt groter terwijl de middenklasse geleidelijk verdwijnt.	Technologie en klimaatverandering ontwrichten de manier waarop we leven en functioneren als individu, organisatie en maatschappij.	De demografische druk op bedrijven, sociale instituties en de economie neemt toe.	De internationale consensus brokkelt af terwijl nationalisme en populisme groeit.	Het vertrouwen in instituties en technologie neemt af.
Daardoor:	- neemt de ongelijkheid in kansen toe en sociale mobiliteit af; - raken kansarme regio's verder achter; - worden traditionele geldbronnen (bijvoorbeeld spaargeld, pensioenvoorziening) kleiner; - zorgt het verschil in toegang tot technologische mogelijkheden voor nog grotere ongelijkheid.	- moeten bedrijven hun bedrijfsmodellen voortdurend aanpassen; - moeten bedrijven rekening houden met tekorten aan productiemiddelen, grondstoffen, waardevermindering van activa en verstoringen in de toeleveringsketen. - worstelen instituties (bijvoorbeeld onderwijs, overheden) met aanpassingen en lopen zij het risico daarin te falen; - vindt er een grote transformatie van werk plaats door automatisering, waarbij veel traditionele banen verdwijnen; - verandert de relatie tussen mens en technologie voortdurend; - bepaalt technologische kapitaal het verschil tussen succes en mislukking;	- ontstaan er wereldwijd grote verschillen in consumptiepatronen; - krijgen we te maken met grote tekorten op de arbeidsmarkt; - ontstaan ongelijke mogelijkheden voor ontwikkeling tussen landen, onder andere langs de factoren arbeid en kapitaal; - ontstaan er in oude economieën problemen met de financiering van oudedagsvoorzieningen waardoor mensen pas later met pensioen kunnen; - staan jonge economieën voor de uitdaging om op grote schaal banen te creëren voor met name jonge mensen.	- verdringen acute lokale zorgen mondiale problemen; - neemt de maatschappelijke tegenstelling toe; - Concurrentie tussen landen ('wie is het beste') neemt toe; - Focust politieke besluitvorming steeds meer op de regio.	- brokkelt de reputatie af van instituties die de steunpilaren vormden van de maatschappij en neemt het draagvlak voor regels af. - neemt het vertrouwen in persoonlijke en digitale veiligheid af; - groeit het wantrouwen tegen mensen die niet tot de 'eigen' groep behoren; - groeit de scepsis tegenover de voordelen die veranderingen kunnen brengen; - vindt steeds meer een debat plaats over wat waar en niet waar is.

1. Toetsen strategische besluitvorming

- 1. Commissie
- 2. Continuïteit
 - 1. Toetsen strategische besluitvorming
 - 2. Beoordelen strategie, business- en investeringsplannen
 - 3. Monitoren van het waardecreatieproces
 - 4. Signaleren van risico's
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De Code verlangt een nauwe betrokkenheid van de raad van commissarissen bij de strategie, die gericht moet zijn op duurzame langetermijnwaardecreatie:

- Het bestuur betreft de raad van commissarissen tijdig bij de formulering van de strategie.
- Het bestuur legt verantwoording af aan de raad van commissarissen over de strategie en de toelichting daarop.
- De raad van commissarissen houdt toezicht op de manier waarop het bestuur de strategie uitvoert en bespreekt regelmatig de strategie en de uitvoering, net als de bijbehorende risico's.
- De raad van commissarissen legt hierover extern verantwoording af in het eigen verslag in het jaarverslag.

Koers regelmatig heroverwegen

Bij de strategiebepaling wordt volgens de Code onder meer aandacht besteed aan:

- haalbaarheid en implementatie;
- bedrijfsmodel en markt;
- kansen en risico's;
- operationele en financiële doelen (en de invloed daarvan op de toekomstige marktpositie).

De strategie is niet in beton gegoten: de koers moet regelmatig worden herijkt aan de dynamiek in de markt, nieuwe technologische ontwikkelingen en andere businessmodellen. Hierbij kan gedacht worden aan de megatrends zoals hiervoor besproken. Dat kan noodzaken tot aanpassingen op korte termijn van de langetermijnstrategie.



De rol van de auditcommissie

Betrokken zijn bij en toezicht houden op de strategie is een taak van de gehele raad van commissarissen. De auditcommissie kan daarin een belangrijke voorbereidende en ondersteunende rol spelen met:

- een kritische toetsing van de levensvatbaarheid en een goede onderbouwing van strategie of businessplan en de financiering daarvan;
- het inschatten van de risico's en de gevolgen voor de continuïteit op de korte en lange termijn;
- het evalueren van het risicomanagement ten aanzien van de geïdentificeerde risico's en de interne beheersing hierop;
- het beoordelen van de aanwezigheid en kwaliteit

Dilemma: betrokkenheid versus afstand

De raad van commissarissen moet volgens de Code zowel een bijdrage leveren aan de formulering van de strategie als toezicht houden op de uitvoering daarvan. Dat plaatst raden van commissarissen voor een dilemma: intensieve betrokkenheid bij de strategie maakt het lastig om daarover later een onafhankelijk oordeel te vellen. Commissarissen zullen dus de juiste balans moeten zien te vinden in hun bemoeienis met de strategie en deze zoveel mogelijk willen objectiveren. De auditcommissie kan bijdragen aan een onafhankelijke opstelling door de raad van commissarissen te voeden met kritische vragen voor een stevige discussie met het bestuur over de (cijfermatige) onderbouwing van strategische plannen, de bijbehorende risico's, de uitvoering van de strategie en de noodzaak van eventuele bijsturing. Het bestuur stelt dus de strategie op en wordt daarover bevraagd door de raad van commissarissen. Het bestuur gaat daarna met huiswerk verder om tot een finale strategie te komen. Op deze manier kan de auditcommissie bijdragen aan het bewaken van de balans tussen betrokkenheid en afstand voor de raad van commissarissen.

van strategische scenarioplanning en een zorgvuldige monitoring van de uitvoering van de strategie.

Dat is ook conform de Code: deze verlangt dat de auditcommissie zich in het toezicht onder meer richt op de financiering van de vennootschap. Verder eist de Code dat de auditcommissie verslag uitbrengt aan de raad van commissarissen over onder meer:

- de uitvoering van de beoordeling, beheersing en monitoring van risico's die zijn verbonden aan de strategie en;
- de materiële risico's en onzekerheden die relevant zijn voor de verwachting van de continuïteit van de vennootschap voor

de komende twaalf maanden, evenals de toekomstbestendigheid van de organisatie.

Ook cultuur(verandering) monitoren

Daarnaast stelt de Code dat de cultuur van de organisatie eveneens gericht is op duurzame langetermijnwaardecreatie. Het bestuur geeft deze cultuur vorm, de raad van commissarissen houdt daar toezicht op. Ook hier ligt een rol voor de auditcommissie: het in kaart laten brengen van de bestaande cultuur en het verschil met de gewenste cultuur en de risico's die daaraan zijn verbonden voor duurzame langetermijnwaardecreatie, plus de monitoring van een eventuele cultuurverandering. Dat onderwerp komt uitgebreid aan de orde in hoofdstuk 5.

2. Beoordelen strategie, business- en investeringsplannen

1. Commissie

2. Continuïteit

1. Toetsen strategische besluitvorming
2. Beoordelen strategie, business- en investeringsplannen
3. Monitoren van het waardecreatieproces
4. Signaleren van risico's

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Auditcommissies richten zich primair op het lopende boekjaar: de jaarrekening, het resultaat en de kwaliteit van het verslagleggingsproces. De Code vraagt om nog meer aandacht voor de lange termijn: auditcommissies staan voor de uitdaging om naast hun focus op de korte termijn en de continuïteit van de organisatie ook de waardecreatie op de lange termijn in acht te nemen. De auditcommissie moet het bestuur daar kritisch over bevragen.

Ook naar bedreigingen kijken

Het hebben van goede checks & balances aan de voorkant van strategische beslissingen is cruciaal. Visionaire ondernemers zijn van nature optimistisch en kijken liever naar kansen dan naar bedreigingen. Te vaak ontbreekt scenarioplanning met what-ifs scenario's waarop kan worden teruggevallen als de verwachtingen niet worden waargemaakt. Ook kan er sprake zijn van dynamiek tussen de ceo en de cfo rondom financiering of **risk appetite** (risicobereidheid). Daarnaast is een cruciale vraag of de financiering van het businessplan gewaarborgd is, ook in een what-ifs scenario.

■ De rol van de auditcommissie

Het is de taak van de auditcommissie om het bestuur kritisch te bevragen over de financiële onderbouwing van de strategische plannen en een goede onderbouwing te eisen, met verifieerbare uitgangspunten en aannames, evenals scenarioanalyses in de vorm van een optimistisch, een realistisch en een pessimistisch scenario. Dat helpt de raad van commissarissen

Best practices voor beoordelen strategische plannen

- Neem geen genoegen met (alleen) intuïtie of beperkte informatie.
- Eis een goede kwantitatieve én kwalitatieve onderbouwing.
- Vraag door op de gehanteerde aannames en uitgangspunten.
- Vraag naar de risico's: worden die goed benoemd en inzichtelijk gemaakt?
- Vraag naar alternatieven; wat als het plan niet volledig gerealiseerd wordt of als er sprake is van tegenvallers? Hoe gevoelig is de prognose hiervoor en hoe denkt de directie hier dan mee om te gaan?
- Eis naast een managementcase ook een sensitized case, op basis van een minder optimistisch scenario.
- Vraag hoe tussentijds kan worden bijgestuurd.

bij een objectieve beoordeling van de plannen, het stellen van de juiste vragen en het verbeteren van de kwaliteit van de strategische besluitvorming. Hierbij mag de financiering van de plannen niet vergeten worden.

Beoordelen levensvatbaarheid en financiering van het plan

Bij de beoordeling van strategische plannen, businessplannen en investeringsvoorstellen staan twee zaken centraal:

Voorbeelden van praktijkvragen door de auditcommissie:

Investeringsplan – Het bestuur presenteert een investeringsplan van miljoenen euro's. Vraagt de auditcommissie naar een gedegen onderbouwing om de haalbaarheid te kunnen inschatten?

Businessplan – Het gepresenteerde businessplan weerspiegelt de groeiambitie door het extrapoleren van de cijfers: meer winst, een stijgende omzet en dalende kosten. Kent de auditcommissie het verhaal achter de cijfers: is de groeiambitie reëel? Wat zijn de echte waardedrijvers? Welke externe factoren beïnvloeden omzet, marge en kosten? Is het plan volledig gefinancierd, ook in een what-ifs scenario? Welke risicoverlagende maatregelen zijn mogelijk indien alternatieve scenario's zich voordoen? Hoe snel kan er bijgestuurd worden?

Budget – De organisatie is volledig gericht op het jaarlijkse budget. Vraagt de auditcommissie aan het bestuur of ook gekeken wordt naar de onderliggende businessplanningcyclus en het langetermijnplan en de noodzaak tot bijstelling daarvan als gevolg van externe ontwikkelingen?

• toekomstbestendigheid

- strategisch, duurzaam, commercieel en operationeel
- haalbaar en berekend op tegenvallers
- op korte termijn en lange termijn

• financiering

- waterdichtheid: hoe zeker is de financiering?
- op korte en lange termijn
- welke kritische voorwaarden zijn er gesteld? (convenanten)
- hoe groot is de verwachte ruimte hierin, nu en in de toekomst?

Het businessplan en de financiering moeten met elkaar in evenwicht zijn, op zowel de korte als de lange termijn. Anders komt de continuïteit onder druk te staan. Er is bijvoorbeeld sprake van financiële of operationele onevenwichtigheid wanneer er tegenover de investeringen aan de linkerkant van de balans onvoldoende financiering aan de rechterkant van de balans staat, of wanneer de resultaten tegenvallen, terwijl er wel aan harde aflossingsverplichtingen moet worden voldaan. Beide situaties hebben een negatieve invloed op de cashflow. Als dit structureel het geval is, kan het voortbestaan van de organisatie ernstig in gevaar komen. De auditcommissie beoordeelt of er sprake is van

1. Commissie

2. Continuïteit

- 1. Toetsen strategische besluitvorming
- 2. Beoordelen strategie, business- en investeringsplannen
- 3. Monitoren van het waardecreatieproces
- 4. Signaleren van risico's

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

dergelijke bedreigingen en dus of er sprake is van een levensvatbaar en volledig gefinancierd plan.

Simpele rekensommen

Dat klinkt simpel en dat is ook meteen een best practice: benader de beoordeling van strategische plannen/businessmodellen zo simpel en praktisch mogelijk. Maak toekomstverwachtingen zo concreet mogelijk en vertaal een complex plan in een aantal overzichtelijke kpi's (key prestatie-indicatoren). Een simpel rekensommetje biedt vaak meer inzicht dan een gedetailleerde en daardoor ingewikkelde winst-en-verliesrekening.



Businessplan

- proces van het businessplan en prestaties in het (recente) verleden
- belangrijkste kasstroomgenererende aspecten van het businessplan
- operationele verbeterplannen
- belangrijkste kwetsbaarheden, gevoeligheden en kansen
- ruimte in de liquiditeit
- minimaal benodigde operationele kasstroom
- seizoensgebondenheid
- de omgeving en onrust
- maatregelen – acties voor verbetering

Best practice

Bij de continuïteit van de onderneming draait alles om cash. Auditcommissies kunnen daarbij de volgende vragen stellen: is er sprake van een robuust gefinancierd businessplan? En: is er voldoende grip op de cashflow, op de ingaande en uitgaande geldstromen? Is er grip op elementen die van invloed kunnen zijn op bankconvenanten zoals financiële ratio's? Is er voldoende cash, maar ook: is er voldoende bewegingsruimte binnen de geldende financieringsafspraken?



Financiering

- soort(en) van financieringsovereenkomst
- wat wordt gezien als wanbetaling, convenanten, cross-defaultclausules
- mechanismen voor het repareren van het eigen vermogen, clear-downbepalingen en een verbod op financiering door derden
- afspraken tussen de financierende partijen
- onderlinge verwevenheid en onderlinge afhankelijkheid
- monitoringsprocedure
- voortzetten of intrekken van faciliteiten
- de noodzaak voor een garantie
- de stakeholderdynamiek

Drie rekenvoorbeelden voor beoordeling strategische doelstellingen

Voorbeeld 1: Investeringsvoorstel van vijftig miljoen euro voor internationalisering

Een bedrijf is mondiaal actief in een markt van 200 miljoen euro. Het bestuur vraagt de raad van commissarissen om goedkeuring van een plan voor het investeren van 50 miljoen euro voor het ontwikkelen van nieuwe producten in de komende vijf tot zeven jaar. Loont deze investering?

Antwoord: Een rekensom leert dat het bedrijf de komende tien jaar een marktaandeel van veertig procent moet behalen om de investering terug te verdienen. Dat is niet realistisch. De raad van commissarissen keurt het investeringsvoorstel af.

Voorbeeld 2: Groeidoelstelling in een verzadigde markt

Een beursgenoteerd bedrijf streeft voor de komende jaren naar een omzetvergroting van ruim 2 miljard euro met het bestaande product in thuismarkt Nederland. Het bestuur wil daarmee tegemoetkomen aan de hooggespannen verwachtingen van de aandeelhouders. Een realistische strategie?

Antwoord: Nederland telt 18 miljoen inwoners. Circa de helft daarvan is al klant bij het bedrijf. De omzetvergroting moet dus bij de overige 9 miljoen inwoners gerealiseerd worden. Dat komt per nieuwe klant neer op een gemiddelde besteding van 200 tot 300 euro per maand. Daarmee is de groeidoelstelling onhaalbaar.

Voorbeeld 3: Omzet- en margevergroting

Een bedrijf realiseert momenteel 100 miljoen euro omzet en wil binnen vijf jaar doorgroeien naar 120 miljoen euro. Tegelijkertijd wil het bestuur de marge verbeteren van vijf naar zes procent. Is dat haalbaar?

Antwoord: De doelstellingen lijken haalbaar. Voor een goede beoordeling zal de auditcommissie het bestuur echter vragen naar een gedegen onderbouwing:

- Wat is de visie op het volume van de (wereld)markt?
- Hoe wil het bestuur marktaandeel en die ene procent margeverbetering winnen?
- Welke investeringen moeten daarvoor worden gedaan?
- Welke invloed heeft de margeverbetering op het aantal eenheden verkocht product?

3. Monitoren van het waardecreatieproces

1. Commissie
2. Continuïteit

1. Toetsen strategische besluitvorming

2. Beoordelen strategie, business- en investeringsplannen
3. Monitoren van het waardecreatieproces
4. Signaleren van risico's
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis
9. Communicatie

De raad van commissarissen wordt niet alleen betrokken bij de formulering van de strategie, gericht op duurzame langetermijnwaardecreatie, maar houdt ook toezicht op de uitvoering daarvan. De auditcommissie speelt daarbij een belangrijke rol.

Monitoren waardecreatieproces

Voor het tijdig (bij)sturen van de uitvoering van de strategie of het businessplan is een strakke monitoring van het waardecreatieproces belangrijk: waar staat de organisatie ten aanzien van het realiseren van de strategische doelstellingen voor de lange termijn? De auditcommissie kan goed zicht krijgen op de voortgang met behulp van het waardecreatiemodel: een overzicht van het waardecreatieproces, vertaald naar een set van passende (en meetbare) financiële en niet-financiële kpi's voor het scheppen van waarde op de lange termijn. Is er voldoende balans in de kpi's en dekken die het gehele waardecreatieproces af?

Daarbij kan het waardecreatiemodel zoals in de figuur rechts worden gehanteerd.

De rol van de auditcommissie

Het is aan de auditcommissie om het bestuur kritisch te bevragen over de prestaties op het gehele spectrum van financiële en niet-financiële kpi's, aan de hand van de interne rapportages daarover. Daarnaast kan de auditcommissie zelf onderwerpen agenderen en informatie aan het bestuur vragen. Bestuurders

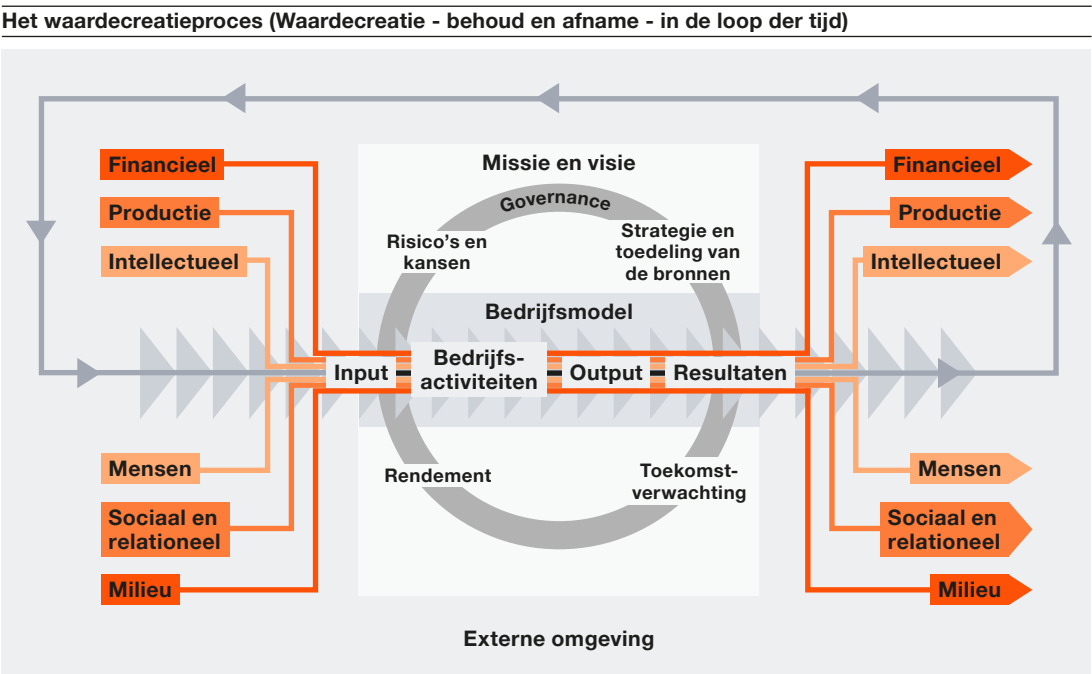
hebben niet altijd een objectief of realistisch antwoord op die vragen. Soms is de interne organisatie daar onvoldoende op ingericht, soms ook hebben bestuurders zich volledig geïdentificeerd met 'hun' strategie en lijden ze aan tunnelvisie.

Voorbeeldvragen

- Is de organisatie in staat om de doelstellingen voor de lange termijn te realiseren: hoe verhouden de werkelijke resultaten zich tot de prognoses?
- Presteert de organisatie daarbij beter of slechter dan de markt?
- Welke verschillen tussen de werkelijke performance en het jaarlijks budget vallen op, maar vooral ook in de vergelijking van het meerjarenplan met de gerealiseerde resultaten? Neem geen genoegen met ontwijkende antwoorden, maar vraag dóór.
- Wordt er over de gehele linie goed of juist slecht gescoord, of geldt dat in het bijzonder voor bepaalde kpi's?
- Wat zijn achterliggende/structurele oorzaken voor achterblijvende prestaties?
- Wat zeggen de prestaties over de redelijkheid van de aannames voor de toekomstige resultaten en over de houdbaarheid van de strategie?
- Is bijsturen noodzakelijk en zo ja: op welk gebied?

Alternatieve informatiebronnen

Bij de monitoring van de uitvoering van de strategie, stellen proactieve auditcommissies zich niet afhankelijk op van het bestuur.



Ze gaan zelf op zoek naar alternatieve informatie uit andere bronnen binnen en buiten de organisatie, zoals leden van het executive committee, de financiële kolom en andere managers of staffunctionarissen. Daarnaast kunnen ze een beroep doen op (het hoofd) Internal Audit en de externe accountant.

Internal Audit en de externe accountant inzetten

Internal Audit en de externe accountant doorkruisen voor de controles de gehele

organisatie en praten met mensen op alle niveaus: van de werkvloer tot de bestuurskamer. Auditcommissies kunnen hen inzetten als hun ogen en oren. De auditcommissie kan invloed uitoefenen op het werkplan van Internal Audit (en keurt dit plan goed) en daarin bijvoorbeeld de monitoring van de uitvoering van de strategie opnemen en daarover laten rapporteren. Hetzelfde geldt voor het signaleren van risico's die aan de strategie zijn verbonden. Zie voor informatievergaring ook hoofdstuk 8.

1. Commissie

2. Continuïteit

1. Toetsen strategische besluitvorming
2. Beoordelen strategie, business- en investeringsplannen
3. Monitoren van het waardecreatieproces
4. Signaleren van risico's

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

4. Signaleren van risico's

Structureel achterblijvende resultaten, plus risico's en onzekerheden (zowel financieel als niet- financieel) kunnen het waardecreatieproces in gevaar brengen en zelfs het voortbestaan van de organisatie bedreigen. Een kernvraag voor auditcommissies luidt dan ook: is de continuïteit van de organisatie gewaarborgd, zowel bij het formuleren als het uitvoeren van de strategie, het businessplan of het investeringsvoorstel?

Wel of geen continuïteitsvraagstuk?

De Code heeft een belangrijke plaats ingeruimd voor continuïteit en transparantie over de risico's en onzekerheden die deze kunnen bedreigen. Graag verwijzen we hiervoor ook naar Hoofdstuk 4.5: Interne en externe verantwoording. Zo wordt het bestuur in het bestuursverslag geacht te verklaren dat de financiële verslaggeving is opgesteld op basis van de continuïteitsveronderstelling. Voorheen hoefde alleen een toelichting in de jaarrekening te worden opgenomen als de inherente continuïteitsveronderstelling van de financiële overzichten werd ondermijnd door risico's en onzekerheden van materieel belang. Die continuïteitsveronderstelling impliceert dat de organisatie in staat is om de activiteiten in de 'voorzienbare toekomst' voort te zetten, de gerapporteerde activa te realiseren en de verplichtingen na te komen. Het bestuur legt in het going concern-memo uit op welke punten de continuïteit onder druk staat en welke maatregelen worden genomen om deze veilig te stellen. De Code verlangt dat het bestuur nu ook standaard in het bestuursverslag expliciet verklaart

dat er sprake is van een continuïteitssituatie en anders aangeeft waarom dit niet het geval is.

Risico's voor de continuïteit in de komende twaalf maanden

Daarnaast moet het bestuur in het verslag vooruitblikken op de risico's en onzekerheden die relevant zijn voor de continuïteit voor de twaalf maanden na het opmaken van de jaarrekening, aldus de Code. De auditcommissie brengt over dit laatste verslag uit aan de raad van commissarissen, samen met de eigen bevindingen. Auditcommissies die vooroplopen op het gebied van governance zullen hierover wellicht ook extern verantwoording willen afleggen in het jaarverslag (als onderdeel van het verslag van de raad van commissarissen). (Zie daarvoor ook hoofdstuk 9.)

Alert zijn op waarschuwingssignalen

Auditcommissies moeten voor het inschatten van strategische, operationele en financiële risico's en onzekerheden alert zijn op waarschuwingssignalen: vroege signalen dat de continuïteit van de organisatie in gevaar kan komen.





Corporate impact

Maatschappelijke waardecreatie

03

3. Corporate impact - maatschappelijke waardecreatie

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
 - 1. Corporate impact integreren in de strategie
 - 2. Corporate impact integreren in de bedrijfsvoering
 - 3. Corporate impact integreren in de verslaglegging
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Organisaties worden in toenemende mate aangesproken op hun maatschappelijke verantwoordelijkheid. De samenleving vraagt om meervoudige waardecreatie voor een bredere groep stakeholders dan alleen de aandeelhouder met een langetermijnfocus. De rol van de auditcommissie ligt op het terrein van strategisch risicobeheer, compliance, duurzaamheid en geïntegreerde verslaglegging.

Bij meervoudige waardecreatie gaat het niet langer alleen om **profit** (aandeelhouderswaarde), maar ook om **people** (sociaal verantwoord ondernemen met inachtneming van de medewerkers, de keten en de samenleving in het algemeen) en om **planet** (het nemen van verantwoordelijkheid in ecologische zin, ter bescherming van natuurlijke hulpbronnen en klimaat). People, planet, profit staat voor een gebalanceerde aansturing van organisaties, met het doel om duurzame en gedeelde waarde te creëren voor alle belanghebbenden en een positieve invloed

(impact) uit te oefenen op de maatschappij (of de negatieve impact zoveel mogelijk te beperken). Tegenwoordig wordt voor duurzaamheid vaak de terminologie ESG gebruikt: Environment, Social en Governance. Denk hierbij aan de nieuwe EU-wetgeving, omtrent verslaglegging, de Corporate Sustainability Reporting Directive (CSRD), waarin organisaties wordt gevraagd om over hun belangrijkste impact, risico's en kansen (IRO's)

Uit de praktijk

Het jaarverslag van Randstad omvat een compleet verhaal met een heldere structuur. In het begin van het verslag wordt over meerdere pagina's inzichtelijk het bedrijf met de bedrijfsonderdelen (per land) beschreven. Zo ook is er een mooi overzicht met de wetgeving per land. De marktontwikkelingen zijn uitgebreid toegelicht. Ook ten aanzien van de missie en strategie is een uitgebreide toelichting te vinden. De waardecreatie is in een inzichtelijk hoofdstuk uitgelegd. Verder is er veel aandacht voor verantwoord ondernemen. Er is een eerste aanzet gedaan over hoe Randstad met de zogenoemde CSRD-rapportage om moet gaan en hoe het bedrijf de daarin voorgeschreven dubbele materialiteit toe gaat passen.

Bron: Juryrapport FD Henri Sijthoff-prijs 2024.



In dit hoofdstuk komen de volgende onderwerpen aan de orde:

- 1. Corporate impact integreren in de strategie
- 2. Corporate impact integreren in de bedrijfsvoering
- 3. Corporate impact integreren in de verslaglegging

ten aanzien van ESG-thema's te rapporteren. De zogenoemde dubbele materialiteitsbepaling, waarbij zowel impact als financiële materialiteit wordt bepaald (IRO's), is een belangrijke nieuwe verplichting voor organisaties en vormt de basis van voor organisaties en de basis van de rapportage over ESG.

Oog voor de bredere context

Gedeelde waarde voor alle stakeholders: dat sluit nauw aan bij de wettelijke brede taakstelling van de raad van commissarissen en daarmee ook op de taken en verantwoordelijkheden van de auditcommissie. De raad van commissarissen richt zich op de belangen van alle stakeholders en duurzame langetermijnwaardecreatie.

1. Commissie

2. Continuïteit

3. Corporate impact

1. Corporate impact integreren in de strategie
2. Corporate impact integreren in de bedrijfsvoering
3. Corporate impact integreren in de verslaglegging

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

De Code vult die verantwoordelijkheid explicieter in, zoals al eerder aangegeven in hoofdstuk 2. Van (bestuurders en) commissarissen wordt verwacht dat zij zich richten op duurzame langetermijnwaardecreatie. Bij de bepaling van de strategie wordt aandacht besteed aan de belangen van stakeholders en worden deze zorgvuldig gewogen. Ook vraagt de Code bij de vormgeving van de strategie ‘voldoende oog voor de bredere context’ waarin de organisatie opereert. Daaronder wordt volgens het Besluit bekendmaking niet-financiële informatie verstaan:

- milieu;
- sociale en personeelsaangelegenheden;
- de keten waarin de onderneming opereert;
- eerbiediging van mensenrechten;
- bestrijding van corruptie en omkoping.

Grote OOB's zijn volgens dit besluit verplicht om een zogenoemde ‘niet-financiële informatieverklaring’ in hun jaarverslag op te nemen over deze thema's, plus de belangrijkste risico's en niet-financiële prestatie indicatoren die daarmee gepaard gaan. Als de organisatie geen beleid heeft voor deze onderwerpen, dan moet dit worden uitgelegd, iets wat gezien de huidige ontwikkelingen onwaarschijnlijk wordt geacht. Het bepalen van de **purpose** (het maatschappelijke doel van de organisatie, zie ook hoofdstuk 6: Cultuur en gedrag), het ontwikkelen van een visie op langetermijnwaardecreatie en het formuleren van een daarbij passende strategie waarin duurzaamheid verankerd is: het zijn allemaal onderwerpen die behoren tot de taken en verantwoordelijkheden van de

gehele raad van commissarissen. In de praktijk stellen raden van commissarissen soms een duurzaamheidscommissie in, om hen daarin te ondersteunen. Ook ondersteunt de auditcommissie de raad van commissarissen steeds vaker bij het toezicht op en de voorbereiding van de besluitvorming op dit terrein.

De rol van de auditcommissie

De auditcommissie richt zich in het algemeen op de ondersteuning van de raad van commissarissen ten aanzien van interne beheersing en verslaggeving. Die verantwoordelijkheid strekt zich ook uit tot purpose, duurzame langetermijnwaardecreatie en strategie, inclusief de daarbij gehanteerde brede context en de niet-financiële informatie daarover, waaronder de bijbehorende risico's en niet-financiële indicatoren. Vanuit deze context is dit hoofdstuk geschreven. De focus ligt daarbij op de maatschappelijke verantwoordelijkheid van organisaties en stakeholderbelangen. Elk onderdeel legt eerst uit hoe organisaties deze verantwoordelijkheid kunnen invullen en schetst daarna de mogelijke rol van de auditcommissie daarbij. Voor duurzame langetermijnwaardecreatie in financiële zin en het veiligstellen van de continuïteit op bedrijfsmatig gebied verwijzen we naar hoofdstuk 2: Continuïteit – duurzame langetermijnwaardecreatie.



1. Corporate impact integreren in de strategie

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
 - 1. Corporate impact integreren in de strategie
 - 2. Corporate impact integreren in de bedrijfsvoering
 - 3. Corporate impact integreren in de verslaglegging
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Purpose en kernwaarden formuleren

Het vertrekpunt voor de strategie is het hogere doel dat de organisatie nastreeft (de **purpose**): waartoe is de organisatie op aarde, wat is het bestaansrecht? De **purpose** hangt samen met de maatschappelijke omgeving waarin de organisatie opereert, de belangrijkste issues daarin en de verwachtingen van stakeholders ten aanzien van de rol en verantwoordelijkheid van de organisatie.

Moreel kompas

De **purpose** mag niet alleen bestaan uit een paar mooie woorden, maar is leidend voor het gedrag van de organisatie en alle medewerkers in de dagelijkse praktijk. De **purpose** wordt vertaald in kernwaarden: waar staan we voor en hoe doen we de dingen? De kernwaarden vormen een richtsnoer voor het gedrag: een (moreel) kompas voor het ijken van prioriteiten en beslissingen en het beoordelen van het eigen handelen en dat van anderen (zie hiervoor ook hoofdstuk 6: Cultuur en gedrag).

Uit de praktijk

Kernwaarden uitzendconcern Randstad

Our core values, established in the company’s early days, represent the foundation of our culture. We use them to guide in every decision we make and every action we take.

Core values

to know

We are experts. We know our clients, talent, suppliers and other business partners, and we know that it’s often the details that count the most.

to serve

We succeed through a spirit of excellent service, exceeding the core requirements of our industry.

to trust

We are respectful. We value our relationships and treat people well.

simultaneous promotion of all interests

We see the bigger picture and take our social responsibility seriously. Our business should always benefit society as a whole.

striving for perfection

We always seek to improve and innovate. We are here to delight our clients and talent in everything we do, right down to the smallest detail.

Bron: [Annual report Randstad 2024](#).



De 17 duurzame ontwikkelingsdoelen (SDG's)

In september 2015 is door de Verenigde Naties een mondiale duurzame ontwikkelingsagenda voor het jaar 2030 vastgesteld. Deze agenda bevat zeventien mondiale doelen, uitgewerkt in 169 subdoelen; zoals het beëindigen van armoede, het verminderen van ongelijkheid en het bestrijden van klimaatverandering. Aan ondernemingen is de oproep gedaan om in belangrijke mate bij te dragen aan het behalen van de doelstellingen.



Uit de praktijk

Purpose lichtproducent Signify

‘Our purpose is to unlock the extraordinary potential of light for brighter lives and a better world. We achieve this through living our values, innovation, passion for sustainability and desire to transform people’s lives.

Bron: [Signify.com](#)

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
 - 1. Corporate impact integreren in de strategie
 - 2. Corporate impact integreren in de bedrijfsvoering
 - 3. Corporate impact integreren in de verslaglegging
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

In kaart brengen maatschappelijke context

De duurzame ontwikkelingsdoelen (Sustainable Development Goals, verder: SDG's, zie kader vorige pagina) blijven een nuttige bron om de doelstellingen die geformuleerd worden voor de meest materiële ESG-onderwerpen. De SDG's geven mondiale ambities voor duurzaamheid die organisaties kunnen gebruiken om deze vervolgens te vertalen naar hun organisatie en scoping. We zien in de praktijk dat steeds meer organisaties het proces van de dubbele materialiteit gebruiken als basis voor het bepalen van hun focus, vanwege de invoering van de CSRD (zie de figuur rechts onderin).

Dubbele materialiteit

De dubbele materialiteit betekent het volgende: de impact van de organisatie op duurzaamheidsonderwerpen én de (financiële) impact hiervan op de onderneming. de (financiële) impact van duurzaamheids onderwerpen op de onderneming. Zowel kansen als risico's worden bepaald, zowel op korte als op lange termijn. In de praktijk doorlopen organisaties het proces van dubbele materialiteit om de meest relevante ESG-onderwerpen te selecteren. Vaak focussen organisaties zich op vijf tot vijftien ESG-onderwerpen die het meest materieel voor hen zijn. Over deze onderwerpen moeten moeten CSRD-plichtige organisaties (ESRS-standaarden) rapporteren in het jaarverslag. Binnen deze materiële onderwerpen is het goed om een keuze te maken waarin de organisatie leidend wil zijn en deze

duurzaamheidsambities vervolgens te koppelen aan de SDGs.

Integreren van de ESG-topics in strategie en waardecreatie

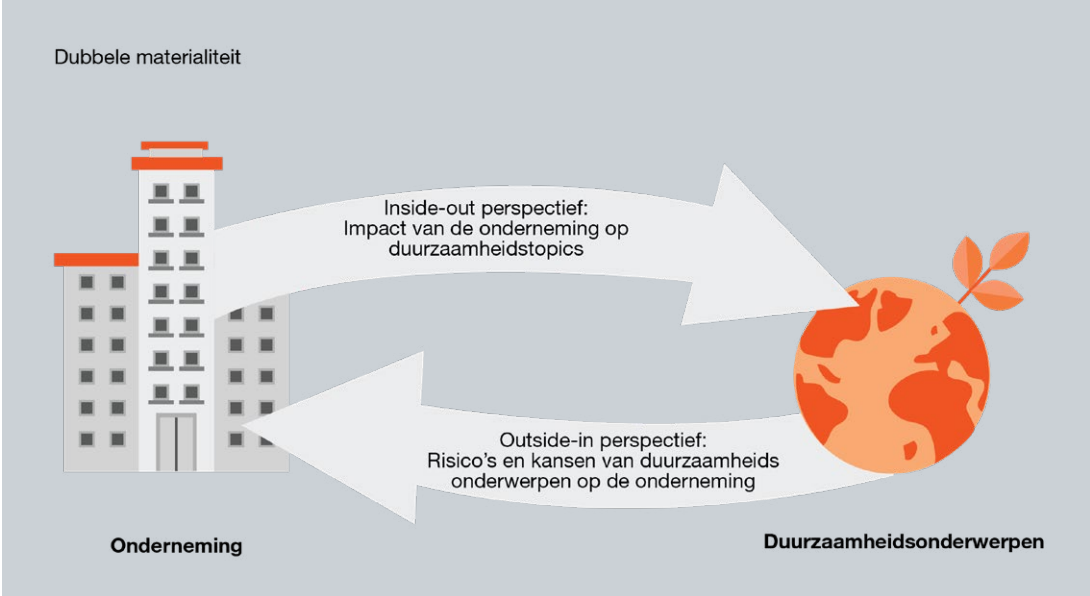
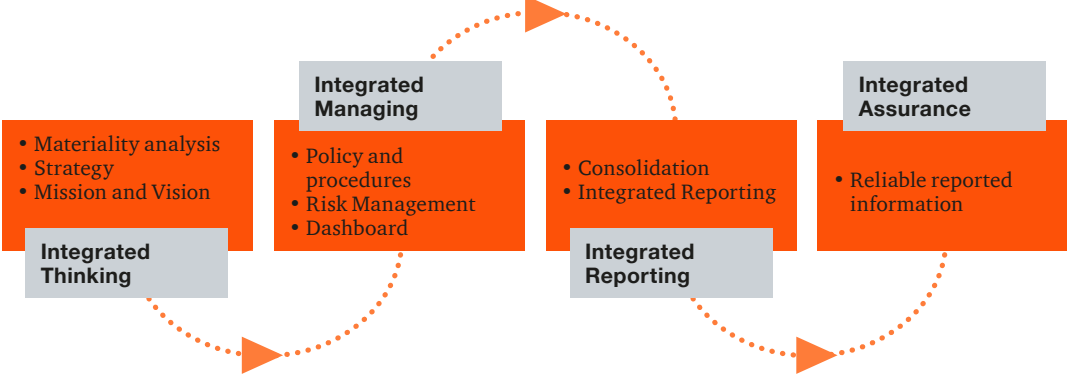
Wanneer de organisatie de impact, risico's en kansen op het gebied van ESG goed in beeld heeft, dan is het belangrijk dat deze geïntegreerd worden in de bedrijfsstrategie en de waardecreatie, zodat er daadwerkelijk kan worden gestuurd op het realiseren van de gecombineerde maatschappelijke en commerciële doelstellingen. Tot slot wordt er extern verantwoording over afgelegd. Het gaat dus om integrated thinking, integrated value creation en integrated reporting (geïntegreerd denken, sturen en rapporteren).

De auditcommissie komt vooral op het vlak van risicobeheer en integrated reporting in beeld.

De rol van de auditcommissie

Discussie over strategische risico's voeren

Vanuit haar rol bij interne beheersing en verslaggeving bereidt de auditcommissie de besluitvorming van de raad van commissarissen voor over het toezicht op de effectiviteit van de interne risicobeheersings- en controlesystemen van de organisatie. De auditcommissie kan het thema maatschappelijke verantwoordelijkheid (bijvoorbeeld via de dubbele materialiteit) dan ook aangrijpen voor een robuuste discussie met het bestuur over de risico's van ontwikkelingen in de maatschappelijke context voor het verdienmodel, de strategie en de licence to operate. Het gaat



1. Commissie

2. Continuïteit

3. Corporate impact

- 1. Corporate impact integreren in de strategie
- 2. Corporate impact integreren in de bedrijfsvoering
- 3. Corporate impact integreren in de verslaggeving

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Best practice

Ga als auditcommissie ook de discussie aan met het bestuur over een niet-financieel thema als maatschappelijke impact en de betekenis daarvan voor de langetermijnwaardecreatie, de continuïteit, het strategisch risicobeheer en de verslaggeving. Welke risico's vormen het klimaatakkoord, de energietransitie of de toekomstige schaarste aan grondstoffen voor de organisatie? Of de mensenrechtensituatie in een belangrijk productieland? Of corruptie in een overzeese afzetmarkt? Daag het bestuur uit op deze thema's. En hoe zijn deze risico's vertaald in bijvoorbeeld waarderingsposten in de jaarrekening en de verslaggeving over (strategische) risico's in het bestuursverslag?

hierbij dus niet alleen om de impact van de activiteiten op de maatschappij (inside-out perspectief), maar ook om de impact van maatschappelijke ontwikkelingen – zoals klimaatverandering – op de onderneming (het outside-in perspectief).

De vragen die de auditcommissie kan stellen in haar voorbereidende rol:

- Maakt het bestuur een systematische analyse van de maatschappelijke context waarin de organisatie opereert?
- Sluiten de **purpose** en de waarden van de organisatie (nog steeds) aan op de maatschappelijke context en verwachtingen?
- Voeren de bestuurders een structurele en dynamische dialoog met elkaar en de raad van commissarissen over de maatschappelijke impact op het verdienmodel en de strategie?
- Welke risico's en kansen brengt de maatschappelijke context mee voor langetermijnwaardecreatie en continuïteit?

- Op welke wijze is de maatschappelijke impact geïntegreerd in de interne risicobeheersings- en controlesystemen en welke acties worden genomen om de geïdentificeerde risico's te beperken?
- Welke (ESG-)rapportageframeworks en -standaarden zijn verplicht en welke verplichtingen komen er nog aan?
- Welke (ESG-)rapportageframeworks worden gebruikt en hoe worden deze keuzes onderbouwd?
- Welk type (ESG-) informatie is key voor aandeelhouders en stakeholders en hoe speelt het management hierop in?
- Op welke (niet-financiële en ESG-) kpi's wordt gestuurd en verantwoording afgelegd? En hoe weet het bestuur dat die informatie betrouwbaar is? (In de praktijk is deze (niet-financiële) informatie vaak afkomstig uit een veelheid van bronnen en systemen, die vaak los staan van de reguliere financiële informatievoorziening.)

Alert zijn op toenemende compliance-risico's

De maatschappelijke dynamiek weerspiegelt zich in nieuwe wet- en regelgeving. Daarnaast worden stakeholderverwachtingen en de politiek-maatschappelijke agenda bepalend voor de verhoudingen in de waardeketen en de toeleveringsketen. De SDG's beïnvloeden (nationale) wetgeving op maatschappelijk gebied en leiden tot incentives of juist uitsluitingen in de internationale keten: met welke partij wordt niet (langer) of juist wel zaken gedaan, omdat deze zich niet volgens de maatschappelijke normen gedraagt, of zich op dat gebied juist proactief opstelt en zich positief onderscheidt? De Europese commissie houdt hier rekening mee in de Green Deal en het Fit for 55-pakket. De auditcommissie zal dus alert moeten blijven op naleving van (nieuwe) wet- en regelgeving en het voldoen aan de vigerende maatschappelijke normen. De gevolgen van niet-naleving voor de bedrijfsvoering zijn immers groot, ook omdat er door de maatschappij sterk op kan worden gereageerd. Nieuwe wetgeving vanuit Europa, zoals de CSRD vraagt expliciet om inzicht in en verantwoording over de toeleverings- en afnemersketen. (Zie hoofdstuk 7: Corporate Reporting.)

Stakeholderengagement in de praktijk brengen

Naast een grondige analyse van de impact, risico's en kansen op het gebied van duurzaamheid, is het verstandig om de behoeften en belangen van stakeholders te analyseren: welke issues vinden zij belangrijk, welke rol verwachten ze van de organisatie en vinden ze dat de organisatie die

verwachtingen wel of niet waarmaakt? Wet- en regelgeving als de CSRD vraagt organisaties om een toelichting in het jaarverslag over hoe ze hun stakeholders kiezen en hoe ze met hen interacteren. Andere wetgeving en standaarden die het belang van stakeholderengagement benadrukken: Corporate Sustainability Due Diligence Directive (CSDDD), UN Guiding Principles, OECD Guidelines for Multinational Enterprises en Global Reporting Initiative (GRI).

Toezicht op stakeholderengagement is een taak van de gehele raad van commissarissen. Mede gezien de toezichtrol van de auditcommissie op het bestuursverslag, is het relevant om inzicht te verkrijgen in het proces van stakeholderengagement. Stakeholderengagement kan in de praktijk op uiteenlopende manieren worden

Best practice

Normen en waarden veranderen voortdurend. Gedrag dat vandaag nog wordt gezien als maatschappelijk verantwoord, kan morgen niet langer geaccepteerd worden door de samenleving. Kijk dus vooruit naar trends en toekomstige issues. Het is van belang de geest van wet- en regelgeving te doorgronden en de toekomstvastheid van voorgestelde acties en maatregelen doorlopend te evalueren.

1. Commissie

2. Continuïteit

3. Corporate impact

- 1. Corporate impact integreren in de strategie
- 2. Corporate impact integreren in de bedrijfsvoering
- 3. Corporate impact integreren in de verslaglegging

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

vormgegeven. In deze publicatie werken we een van die manieren verder uit.

Stakeholders definiëren

Organisaties kunnen eerst helder definiëren wie hun stakeholders precies zijn. Daarbij wordt in de CSRD onderscheid gemaakt tussen **affected** stakeholders en **users of sustainability statements**:

- **Affected stakeholders:** personen of groepen waarvan de belangen positief of negatief (kunnen) worden beïnvloed door de activiteiten van de onderneming en haar directe en indirecte

zakelijke relaties in de gehele waardeketen, bijvoorbeeld zakenpartners, klanten, werknemers en andere werknemers, lokale gemeenschappen, leveranciers en kwetsbare groepen.

- **Users of sustainability statements:** primaire gebruikers van algemene financiële verslaglegging, bijvoorbeeld aandeelhouders en andere investeerders.

Organisaties hebben een aantal stakeholders gemeen. Daarnaast kan elke organisatie eigen, specifieke stakeholders definiëren.

Stakeholderdialoog voeren

De behoeften, eisen en verwachtingen van de verschillende stakeholders zijn divers en dynamisch: ze ontwikkelen zich voortdurend, bijvoorbeeld door een veranderende moraal, maar ook door wijzigingen in wet- en regelgeving. Via een permanente dialoog houdt de organisatie voeling met haar stakeholders en kan worden getoetst of eventuele bijsturing van de purpose, de normen en waarden en de maatschappelijke opstelling gewenst is.

Externe verantwoording afleggen over stakeholderengagement

Het effectief voeren van de stakeholderdialoog vereist ook dat organisaties een transparante en duidelijke externe toelichting geven over de

representativiteit van hun stakeholderengagement en hoe de input van stakeholders wordt meegenomen in het bepalen van materiële onderwerpen, strategie, beleid en bedrijfsmodel. Dit verhoogt de geloofwaardigheid van het jaarverslag en versterkt de relatie tussen organisatie en stakeholders.

Organisaties leggen idealiter in het jaarverslag verantwoording af over het proces voor stakeholderengagement en de belangrijkste uitkomsten daarvan:

- Welke stakeholdergroepen zijn gedefinieerd?
- Hoe vaak en op welke manier is met welke stakeholdergroep contact gezocht?
- Vertegenwoordigt de verzamelde informatie voldoende de belangen van alle stakeholders?
- Welke (materiële) thema's en zorgen hebben stakeholders naar voren gebracht en hoe is de organisatie daarmee omgegaan?

Uit de praktijk

Transparantie over input van stakeholders

“[...] naast inzicht in de uitkomsten van het stakeholder-engagement-proces, duidelijk aan wat de ontvangen boodschappen zijn geweest van de verschillende stakeholders. Daarnaast blijkt uit ‘what they tell us’ wat voor input de stakeholders hebben op de duurzaamheidsprestaties van Ahold Delhaize over de verschillende duurzaamheidsonderwerpen zoals klimaatverandering en mensenrechten. Door inzicht te geven in welke input Ahold Delhaize heeft ontvangen van de verschillende groepen stakeholders, krijgt de gebruiker van het jaarverslag ook een beter inzicht in de relatie tussen de ontvangen boodschappen van de stakeholders en wat hun verwachtingen zijn van Ahold Delhaize als onderneming.”

Bron: 10 navigatiepunten voor CSRD - AFM

Koninklijke Ahold Delhaize (bestuursverslag 2023)



Drie stappen voor het opstellen van een materialiteitsanalyse

De verwachtingen en eisen van de stakeholders van organisaties zijn niet alleen verschillend, maar kunnen ook conflicteren. Klanten kunnen andere belangen hebben dan medewerkers of aandeelhouders. Organisaties zullen dan ook prioriteiten toekennen aan de verschillende belangen van hun stakeholders. Dat vraagt om keuzes: welke belangen laten we prevaleren en hoe past dat bij onze **purpose** en onze waarden?

Het is op korte termijn vaak onmogelijk om de belangen van alle stakeholders op hetzelfde moment in dezelfde mate te honoreren. Op de lange termijn vallen de belangen vaker (indirect) samen.

1. Commissie

2. Continuïteit

3. Corporate impact

- 1. Corporate impact integreren in de strategie
- 2. Corporate impact integreren in de bedrijfsvoering
- 3. Corporate impact integreren in de verslaggeving

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

■ De rol van de auditcommissie

Toezicht houden op het proces van stakeholderengagement

De rol van de auditcommissie ten aanzien van het toezicht op het stakeholderengagement door het bestuur vloeit logisch voort uit de twee primaire verantwoordelijkheden: toezicht op de effectiviteit van het risicobeheer en op de integriteit en kwaliteit van de (financiële) verslaggeving. Het is gebruikelijk dat de auditcommissie zowel bij de opzet als de verankering van stakeholderengagement wordt betrokken.

Stakeholderengagement vanuit het oogpunt van risicobeheer

Het tegemoetkomen aan de verwachtingen van stakeholders hangt direct samen met de **purpose** van de organisatie en het streven naar meervoudige waardecreatie. Daarnaast is stakeholderengagement cruciaal voor het verdienen, verkrijgen en behouden van de maatschappelijke **licence to operate** en daarmee voor de continuïteit van de organisatie. Op korte termijn kan deze bedreigd worden door reputatieschade, resulterend in bijvoorbeeld een klantenboycot. Op de langere termijn kan een mismatch met stakeholderbelangen leiden tot een slechte positie op de arbeidsmarkt, in de keten en bij kapitaalverstrekkers, politieke bemoeienis of zelfs het verlies van het maatschappelijke bestaansrecht.

Best practice

Er is een maatschappelijke roep om snellere en intensievere investeringen in duurzaamheid, terwijl kortetermijngerichte aandeelhouders geen genoeg willen nemen met minder rendement en niet willen afzien van hun dividend. Zie als auditcommissie toe op de transparantie over dilemma's in het bestuursverslag en het omgaan met belangentegenstellingen.

Buiten naar binnen halen

De auditcommissie kan via de stakeholderdialogoog ook zélf belangrijke informatie vergaren over de organisatie en de reputatie, de maatschappelijke context en aankomende issues. Wat leeft er in de samenleving, hoe vertaalt zich dat in toekomstige kansen en risico's en is het bestuur zich daarvan voldoende bewust?



Vanuit haar verantwoordelijkheid voor het toezicht op risicobeheer houdt ook de auditcommissie toezicht op het proces voor stakeholderengagement, hoewel het hier bij uitstek gaat om een toezichttaak van de gehele raad van commissarissen.

Stakeholderengagement vanuit het oogpunt van verslaggeving

Daarnaast ziet de auditcommissie toe op transparantie over de manier waarop de organisatie stakeholderbelangen in kaart brengt, weegt en behartigt. Dat sluit naadloos aan op de trendmatige ontwikkeling (ook in wetgeving) om in het bestuursverslag niet alleen te rapporteren over het behalen van financiële doelstellingen, maar ook over niet-financiële thema's, zoals de impact van de organisatie op mens en milieu.

Stakeholderengagement vormt daarvan een belangrijk onderdeel. De auditcommissie ziet dus ook toe op de integriteit en de kwaliteit van de verslaggeving over het aan de orde stellen van en sturen op stakeholderbelangen. (Zie hoofdstuk 7: Corporate Reporting.)

Best practice

Overweeg regelmatig een stakeholderdialogoog bij te wonen. Zie dat niet als een verplicht nummer, maar als een kans om waardevolle inzichten te vergaren over strategische kansen en risico's voor de organisatie.



Strategische relevantie van stakeholderengagement

Naast het voldoen aan wettelijke eisen kan stakeholderengagement de bredere strategie van de organisatie enorm ten goede komen. Onderzoek van PwC onder leidinggevendenden heeft uitgewezen dat het vermogen om vertrouwen op te bouwen en te behouden bij belangrijke stakeholders ook de winstgevendheid verbetert.¹

Stakeholderengagement als strategische waardedrijver:

- input voor strategie en bedrijfsontwikkeling;
- voldoen aan rapportageverplichtingen;
- bouwen aan sterke relaties;
- voldoen aan due diligence-verplichtingen;
- inzicht in opkomende onderwerpen en maatschappelijke verwachtingen.

Door interactie met stakeholders kunnen organisaties impactvol en relevant blijven.

¹ [PwC's 2024 Trust Survey](#).



1. Commissie
2. Continuïteit
3. Corporate impact
 1. Corporate impact integreren in de strategie
 2. Corporate impact integreren in de bedrijfsvoering
 3. Corporate impact integreren in de verslaglegging
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis
9. Communicatie

Toezicht houden op transparantie en integriteit verslaglegging

De auditcommissie ziet erop toe dat de organisatie adequaat en evenwichtig verantwoording aflegt aan de stakeholders. Bevat het jaarverslag toegankelijke informatie over de contacten met stakeholders en het omgaan met hun belangen en verwachtingen? Welke beheersmaatregelen zijn er om te waarborgen dat de informatie compleet is? Toont de organisatie moreel leiderschap door transparantie over dilemma's? Zijn de beschreven dilemma's ook daadwerkelijk het meest klemmend voor de organisatie? Herkennen de raad van commissarissen en de auditcommissie de organisatie in de geschetste dilemma's?



Best practice

Een dubbele materialiteitsanalyse geeft inzicht in de meest relevante duurzaamheidsgerelateerde impact, risico's en kansen voor een organisatie. Een grondige materialiteitsanalyse is opgesteld met input van stakeholders.



Welke vragen stellen over stakeholderengagement?

De auditcommissie kan de volgende vragen stellen over stakeholderengagement, in haar voorbereidende rol richting de raad van commissarissen:

- Is er een goed functionerend proces voor stakeholderengagement?
- Wordt met alle relevante stakeholders een dialoog gevoerd?
- Nemen bestuurders en commissarissen regelmatig persoonlijk deel aan de dialoog?
- Zijn alle belangrijke thema's en verwachtingen van stakeholders in beeld?
- In hoeverre voldoet de organisatie aan verwachtingen van stakeholders?
- Waar is sprake van belangentegenstellingen en dilemma's en hoe gaat de organisatie daarmee om?
- Is bijstelling van **purpose** en strategie noodzakelijk om de continuïteit van de organisatie te waarborgen?
- Wordt voldoende transparant externe verantwoording afgelegd over de stakeholderdialoog en de uitkomsten daarvan, het adresseren van stakeholderbelangen, de afwegingen en dilemma's daarbij en de motivatie voor de uiteindelijke besluitvorming?

Praktisch: Stakeholderdialoog

Er zijn veel verschillende stakeholders om mee te spreken en vormen van stakeholderdialoog, variërend van individuele gesprekken tot groepsengagement, kwalitatieve en kwantitatieve betrokkenheid, evenals overwegingen rond eenmalige of structurele opname van stakeholderengagement in de governancestructuur van de organisatie.

Veel voorkomende vormen van stakeholderdialoog zijn (formeel en informeel):

- interviews
- enquêtes
- multi-stakeholder forum/councils
- panels en informatiesessies met klanten en ketenpartners (plus onderzoeken naar klanttevredenheid)
- medewerkersbijeenkomsten (plus onderzoeken naar medewerkerstevredenheid en betrokkenheid)
- contacten met aandeelhouders/institutionele beleggers;
- contacten met belangengroeperingen, non-gouvernementele organisaties en maatschappelijke organisaties als vakbonden;
- contacten met externe toezichthouders;
- contacten met de (internationale) politiek;
- contacten met opinieleiders en journalisten;
- vertegenwoordiging in brancheorganisatie en internationale organen;
- deelname aan openbare debatten;
- discours via sociale media: fora, bloggers en influencers.



2. Corporate impact integreren in de bedrijfsvoering

1. Commissie

2. Continuïteit

3. Corporate impact

1. Corporate impact integreren in de strategie
2. Corporate impact integreren in de bedrijfsvoering
3. Corporate impact integreren in de verslaglegging

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Meervoudige waardecreatie vertalen in concrete doelstellingen

Wanneer de maatschappelijke context en de stakeholderverwachtingen hebben geleid tot een heldere **purpose** en strategie, is de volgende stap het integreren daarvan in de bedrijfsvoering en de vertaling in concrete doelstellingen voor

Vier succesfactoren voor corporate impact: van strategie naar executie

- Iedereen in de organisatie heeft een rol te spelen: het is niet alleen een verantwoordelijkheid voor de functionaris of afdeling voor duurzaamheid of corporate impact.
- Leiderschap is een sleutelfactor: van de ceo en het senior management wordt verwacht dat zij zich actief inzetten voor het boeken van vooruitgang, waarop even actief toezicht wordt gehouden, door de raad van commissarissen, ondersteund door de auditcommissie.
- Formuleer relevante kpi's als onderdeel van het strategische dashboard van het bestuur om het behalen van de doelstellingen voor corporate impact te monitoren en te rapporteren over de voortgang.
- Hanteer hetzelfde kwaliteitsniveau voor financiële en niet-financiële informatieprocessen en rapportages.

alle functies van de organisatie. Alleen op die manier kan de maatschappelijke belofte worden waargemaakt. Corporate impact wordt zo onderdeel van de reguliere aansturing van de organisatie: het financiële en economische waardecreatieproces wordt daarmee verbreed en omvat ook maatschappelijke waarde.

De rol van de auditcommissie

Waardecreatieproces monitoren

De raad van commissarissen houdt toezicht op de uitvoering van de strategie, de auditcommissie speelt hierbij een voorbereidende rol: waar staat de organisatie ten aanzien van het realiseren van de langetermijndoelstellingen? Op die manier kan zo nodig tijdig worden bijgestuurd of versneld, bijvoorbeeld wanneer de voortgang achterblijft, of wanneer veranderingen in de maatschappij of stakeholderverwachtingen daarom vragen. De organisatie en de auditcommissie kunnen hierbij gebruikmaken van het waardecreatiemodel van de International Integrated Reporting Council (IIRC). Zie verder hoofdstuk 2.

Vraag om meetbare kpi's voor maatschappelijke impact

De belangrijkste thema's waar de organisatie impact op heeft, of waar de maatschappij belangrijke impact op de onderneming heeft, worden voor zover mogelijk vertaald naar meetbare kpi's voor input, activiteiten, outputs, uitkomsten (outcome) en impact om erop te kunnen sturen en toezicht te houden op de



Welke vragen stellen over het meervoudige waardecreatieproces?

De auditcommissie kan de volgende vragen stellen over het meervoudige waardecreatieproces, in haar voorbereidende rol richting de raad van commissarissen:

- Zijn de duurzaamheidsdoelstellingen (bijvoorbeeld de SDG's) geïntegreerd in de strategie, het proces van langetermijnwaardecreatie/de bedrijfsvoering?
- Hoe wordt daadwerkelijk gestuurd op de geformuleerde doelstellingen? Hoe wordt de impact daarvan gemeten: voor welke benadering/raamwerk heeft de organisatie gekozen, nu een standaardbenadering veelal nog ontbreekt?
- Welke doelstellingen zijn al vertaald in meetbare kpi's voor zowel impact als uitkomsten en voor welke doelstellingen zijn nog geen meetbare indicatoren voorhanden en ontbreekt kwantitatieve stuurinformatie?
- Dekken de kpi's of kwalitatieve indicatoren het gehele waardecreatieproces en alle relevante risico's af en bevinden ze zich op het juiste strategische niveau?
- Hoe zijn de kpi's en kwalitatieve prestatie-indicatoren geïntegreerd in de interne rapportages?
- Is het rapportageproces ingericht op niet-financiële en kwalitatieve data?
- Hebben de processen en rapportages dezelfde kwaliteit en worden ze even serieus genomen als de financiële rapportages?
- Worden de indicatoren gemonitord en wordt zo nodig bijgestuurd? In welke documenten en met welke frequentie vindt dit plaats?
- Zijn de kpi's gekoppeld aan de beoordelings- en beloningssystemen?
- Hoe wordt extern verantwoording afgelegd? Er zijn verschillende raamwerken en benaderingen voor (externe) niet-financiële informatievoorziening: welk raamwerk hanteert de organisatie en waarom is hiervoor gekozen en niet voor de andere raamwerken?
- Vanaf welk jaar is de onderneming CSRD-plichtig en hoever is de onderneming met de implementatie ervan?

1. Commissie

2. Continuïteit

3. Corporate impact

1. Corporate impact integreren in de strategie
2. Corporate impact integreren in de bedrijfsvoering
3. Corporate impact integreren in de verslaglegging

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

voortgang. Het is de rol van de auditcommissie om het bestuur kritisch te bevragen over de prestaties op het gehele spectrum aan kpi's en risico's, zowel financieel als niet-financieel en zowel kwantitatief als kwalitatief. Het vragen om en het beoordelen van het strategische dashboard van het bestuur draagt hieraan bij. De auditcommissie daagt het bestuur uit op het maken van de keuze voor de juiste kpi's om de voortgang van de strategie betrouwbaar te kunnen meten. Zo wordt ook gewaarborgd dat het bestuur het beleid tijdig kan bijstellen, wanneer nodig.

Vraag om niet-financiële indicatoren en rapportages

De brede context van meervoudige waardecreatie vraagt om andersoortige informatie, die veelal niet-financieel en kwalitatief van aard is. Om te sturen op meervoudige waardecreatie zal het vaak voorkomen dat er nieuwe prestatie-indicatoren worden geformuleerd en de interne rapportageprocessen worden aangepast. De auditcommissie houdt toezicht op dat proces en bevraagt het bestuur kritisch. Daarnaast kan de auditcommissie dat interne (veranderings) proces ondersteunen door het bestuur uit te dagen ten aanzien van welke niet-financiële informatie gerapporteerd wordt om prestaties te kunnen meten en monitoren. Immers: **What gets measured, gets treasured.**



3. Corporate impact integreren in de verslaglegging

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
 - 1. Corporate impact integreren in de strategie
 - 2. Corporate impact integreren in de bedrijfsvoering
 - 3. Corporate impact integreren in de verslaglegging
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Verantwoording afleggen via ‘integrated reporting’

Welke maatschappelijke impact heeft de organisatie (zowel positief als negatief), welke voortgang is geboekt met het realiseren van de **purpose** en de daarvan afgeleide doelstellingen en hoe is omgegaan met de belangen van de stakeholders? Dat zijn

voorbeelden van vragen die aan de orde komen in de externe verslaglegging.

Samenhangend verslag doen

De organisatie kan verantwoording afleggen in de vorm van aparte duurzaamheidsverslaggeving, maar bij het streven naar meervoudige waardecreatie ligt (de vervolgstap naar) een

Wat is integrated reporting?

Een geïntegreerd rapport bevat een volledig, beknopt en gebalanceerd beeld van de waardecreatie en -vernietiging van een organisatie in brede zin, inclusief duurzaamheid/ESG. Het helpt stakeholders te begrijpen en te beoordelen welke mogelijkheden de organisatie heeft om waarde te creëren en te behouden op de korte, middellange en lange termijn. Bij geïntegreerd rapporteren gaat de organisatie uit van het wat, hoe en waarom:

- de maatschappelijke omgeving en het daarmee samenhangende doel van de organisatie (het waarom);
- de daaruit voortkomende doelen die de organisatie wil bereiken (het wat);
- de vertaling in de strategie en het waardecreatiemodel (het hoe); en:
- de borging daarvan in de organisatie (governance en beloning);
- tot welke prestaties en impact dat heeft geleid;
- wat er wordt verwacht voor de toekomst.

Dat verhaal wordt verteld vanuit de **purpose** als rode draad en benadrukt de samenhang (de ‘integraliteit’) in sturing op financiële en niet-financiële doelen en indicatoren. Een geïntegreerd rapport wordt opgesteld volgens het raamwerk van de International Integrated Reporting Council (IIRC), aan de hand van het waardecreatiemodel. Vanaf het moment dat een onderneming CSRD-plichtig is zullen de Europese Sustainability Reporting Standards (ESRS) de leidraad vormen voor de rapportage. Die standaarden vereisen een duidelijk afgescheiden onderdeel voor het sustainability statement binnen het bestuursverslag.

Zie ook hoofdstuk 7: Corporate Reporting.

integrated report meer voor de hand. Daarin wordt samenhangend verslag gedaan van de strategie en de prestaties op financieel, sociaal en duurzaamheidsgebied. Europese wetgeving (zoals de CSRD en de EU Taxonomie voor duurzame activiteiten) zal duurzaamheidsverslaggeving afdwingen.

■ De rol van de auditcommissie

De auditcommissie monitort de kwaliteit en integriteit van de verslaggeving. Traditioneel ging het daarbij alleen om financiële verslaggeving, tegenwoordig speelt ook het extern afleggen van verantwoording over niet-financiële thema’s een steeds belangrijkere rol, zoals het gevoerde beleid op het gebied van mens, milieu en maatschappij.

Dat impliceert dat de auditcommissie zich bij de monitoring van de kwaliteit en integriteit van de verslaggeving zowel richt op financiële als op niet-financiële informatie: gecombineerd in een **integrated report**, of in aparte verslagen voor het sociale en duurzaamheidsbeleid. Zie ook hoofdstuk 7: Corporate Reporting.

Uit de praktijk

‘De jury mist in een aantal gevallen ook de blik naar buiten. Meer en meer leggen bedrijven uit hoe ze waarde toevoegen, vaak in de vorm van een waardecreatiemodel. Dat is in de beste gevallen ook nog gekoppeld aan de bijdragen van de bedrijven aan de duurzaamheidsdoelen. Maar het kader waarin dit wordt gerealiseerd blijft onderbelicht. Denk aan een toelichting van de markt waarin het bedrijf opereert, de concurrentieverhoudingen en de sterktes en zwaktes in vergelijking tot anderen (de SWOT-analyse).’

Bron: zie voor de Algemene bevindingen pagina 3 en 4 van het juryrapport FD Henri Sijthoff Prijs 2024.





Control & Compliance

Risicobeheersing en interne controle

04

4. Control & Compliance

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelicht
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Adequate risicobeheersing is cruciaal voor langetermijnwaardecreatie en de continuïteit van de organisatie. Dat vraagt om een robuuste dialoog tussen het bestuur en de commissarissen over het aangaan van risico's en de wijze waarop deze worden aangepakt. De auditcommissie ondersteunt de raad van commissarissen bij het toezicht op de effectiviteit van de opzet en werking van de interne risicobeheersings- en controlesystemen.

Ondernemen gaat onvermijdelijk gepaard met risico's en onzekerheden. Ze vormen het spiegelbeeld van strategische kansen voor het creëren van waarde voor de lange termijn en het veiligstellen van de continuïteit. Risico's zijn onlosmakelijk verbonden met gezond ondernemerschap: wanneer er geen risico's worden genomen, loopt de organisatie kansen mis voor het genereren van groei, omzet en winst.

Passende balans tussen kansen en risico's

Goed geleide organisaties hanteren dan ook een passende balans tussen het grijpen van kansen en de risico's die daarmee gepaard gaan. Ze zijn zich bewust van de risico's die kunnen voortvloeien uit de strategie, de aard van de bedrijfsvoering en de primaire processen en proberen deze zo goed mogelijk te beheersen en te monitoren, passend bij de zogenoemde **risk appetite** van de organisatie. In deze publicatie gebruiken we daarvoor de term 'risicobereidheid'. De interne controle is niet gericht op het vermijden van alle denkbare

risico's, wel op het zorgvuldig managen ervan, met behulp van adequate interne risicobeheersings- en controlesystemen. In dit hoofdstuk staan deze zogenoemde **hard controls** centraal. De **soft controls** – een op langetermijnwaardecreatie gerichte organisatiecultuur en gedrag dat aansluit bij de kernwaarden – komen aan bod in hoofdstuk 5.

Goed samenspel vereist

Gedegen risicobeheer vraagt om een goed samenspel tussen het bestuur, de raad van commissarissen en de auditcommissie, evenals goede communicatie met Internal Audit en de externe accountant. De auditcommissie vervult in dat samenspel een spilfunctie. Daarbij blijft toezicht op de in het oog springende voornaamste risico's, de risicobereidheid en het risicobeheer de verantwoordelijkheid van de raad van commissarissen als geheel. De auditcommissie ondersteunt als subcommissie de raad van commissarissen onder meer in het monitoren van het proces van financiële verslaggeving



In dit hoofdstuk komen de volgende onderwerpen aan de orde:

1. beoordelen van de risico's
2. monitoren van de interne risicobeheersings- en controlesystemen
3. afstemmen met Internal Audit
4. afstemmen met de externe accountant
5. interne en externe verantwoording

en in het toezicht op de effectiviteit van de interne risicobeheersings- en controlesystemen. Daarnaast richt de auditcommissie zich op de financiering en de toepassing van informatie- en telecommunicatietechnologie, waaronder cybersecurity en het belastingbeleid. Op al deze toezichtthema's spelen specifieke risico's.

Alert zijn op reputatierisico's

Van de raad van commissarissen en de auditcommissie wordt een brede blik verwacht. Bij belastingen hoort bijvoorbeeld het reputatierisico dat kan voortvloeien uit het niet adequaat inspelen

6. enkele risicocategorieën uitgelicht:

- strategisch
- operationeel
- cybersecurity
- naleving
- integriteitsschending en fraude
- verslaggeving
- corruptie
- fiscaal

op een trend als **sustainable tax**. En bij ICT, data en AI past alertheid op (reputatie)risico's op het gebied van privacy, bijvoorbeeld door het niet voldoen aan regelgeving op dat terrein.

Het eerste deel van dit hoofdstuk schetst hoe de auditcommissie toezicht kan houden op de opzet en werking van de interne controlesystemen om risico's in het algemeen te beheersen. Het tweede deel van dit hoofdstuk biedt een inhoudelijke beschrijving van risicocategorieën waarmee organisaties vaak te maken krijgen en de rol van de auditcommissie daarbij.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Rol bestuur en toezicht bij de interne risicobeheersings- en controlesystemen

Beoordelen, implementeren en monitoren
Risicobeheer valt volgens de Code uiteen in drie deelverantwoordelijkheden: het beoordelen van de risico's die met de strategie en de activiteiten van de organisatie gepaard gaan, het implementeren van adequate interne

risicobeheersings- en controlesystemen en een systematische monitoring daarvan. Het bestuur is verantwoordelijk voor het identificeren en beheersen van risico's. De raad van commissarissen ziet daarop toe, ondersteund door de auditcommissie.



Wie is waarvoor verantwoordelijk?

De **raad van commissarissen** houdt toezicht op de wijze waarop het bestuur de strategie uitvoert en bespreekt regelmatig (ten minste eenmaal per jaar) de strategie, de uitvoering van de strategie en de daarmee samenhangende risico's. De raad van commissarissen richt zich in het toezicht op het beleid en de gang van zaken in de organisatie en op de effectiviteit van de interne risicobeheersings- en controlesystemen van de organisatie.

De **auditcommissie** bereidt de besluitvorming van de raad van commissarissen op het gebied van risicobeheer voor. De auditcommissie monitort de effectiviteit van de interne risicobeheersings- en controlesystemen.

De essentie van toezicht door de auditcommissie op de 'hard controls'

1. begrip van de vastgestelde strategie/doelstelling en de bijhorende risico's en risicobereidheid;
2. inzicht in de risicohouding van de organisatie, onder meer tot uiting komend in de manier waarop de organisatie interne risicobeheersings- en controlesystemen heeft opgezet voor de geïdentificeerde risico's;
3. inzicht in hoe het bestuur de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen toetst en monitort en hierover verantwoording aflegt aan de auditcommissie/raad van commissarissen;
4. toezicht op de opvolging door de organisatie van bevindingen en aanbevelingen ten aanzien van de interne risicobeheersings- en controlesystemen en het identificeren en incorporeren van risico's die ontstaan uit bijvoorbeeld nieuwe ontwikkelingen in de strategie, de wet- en regelgeving en de concurrentie, de maatschappij en de geopolitieke omgeving;
5. toezien of alle significante wijzigingen in de interne risicobeheersings- en controlesystemen en geplande verbeteringen zijn gerapporteerd in het jaarverslag.



1. Beoordelen van de risico's

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

1

Risico-beoordeling

Het bestuur inventariseert en analyseert de risico's die verbonden zijn aan de strategie en de activiteiten van de organisatie. Het bestuur stelt de risicobereidheid vast en besluit welke maatregelen tegenover de risico's worden gezet.

Vaststelling van de risicobereidheid

Een kernbegrip bij het beoordelen en afwegen van de risicostrategie is de risicobereidheid van het bestuur en de raad van commissarissen.

Het bestuur stelt vast in hoeverre het bereid is tot het nemen van risico's. Dat vormt het vertrekpunt voor de interne risicobeheersings- en controlesystemen, die de genomen risico's moeten afdekken.

Risicobereidheid en risicotolerantie

Risicobereidheid is de hoeveelheid risico, op een breed niveau, die een organisatie bereid is te accepteren in het streven naar waarde. Het weerspiegelt de filosofie van de organisatie op het gebied van risicobeheer en beïnvloedt de cultuur van de organisatie.

Zowel risicobereidheid als risicotolerantie stelt grenzen aan hoeveel risico een organisatie bereid is te accepteren.

Risicobereidheid is een uitgangspunt op een hoger niveau en houdt in grote lijnen rekening met de risiconiveaus die het bestuur aanvaardbaar acht. Risicotolerantie vormt een nauwer begrip en bepaalt het aanvaardbare niveau van variatie rond doelstellingen.

Bijvoorbeeld: een bestuur dat zegt dat het geen risico's accepteert die kunnen leiden tot een aanzienlijk verlies van de inkomstenbasis, toont zijn risicobereidheid. Wanneer hetzelfde bestuur zegt dat het geen risico's wil accepteren die ervoor zouden zorgen dat de omzet van de top 10-klanten met meer dan 10% zou dalen, drukt dat de risicotolerantie uit.

Werken binnen risicotoleranties biedt het bestuur meer zekerheid dat de organisatie binnen de risicobereidheid blijft. Dat biedt de organisatie de doelstellingen zal bereiken.

De mate van risicobeheersing en interne controle moet passen bij en in de juiste verhouding staan tot:

- de risicobereidheid van het bestuur;
- de directe en indirecte kosten (investeringen in systemen en mensen, plus beslag op kostbare managementtijd en bureaucratische belasting);
- het soort organisatie (over het algemeen kunnen minder complexe organisaties met minder omvangrijke procedures volstaan).

■ De rol van de auditcommissie

De auditcommissie kan de raad van commissarissen bijstaan in het ontwikkelen van een visie op de risicobereidheid en betreft daarin aspecten als:

- toon aan de top: integriteit en authenticiteit; communicatie van belang en bewustzijn van risicobeheersing naar de rest van de organisatie en de beleving daarvan;
- balans tussen risicoprofiel/bereidheid, impact van de risico's op de bedrijfsvoering en de interne risicobeheersings- en controlesystemen.

Verder ziet de auditcommissie erop toe dat de risicobereidheid wordt geconcretiseerd in het risicomanagement, met procedures die stringent gevolgd moeten worden, zodat de effectiviteit van de interne risicobeheersings- en controlesystemen is gewaarborgd.

Vijf manieren voor het omgaan met risico's

Accepteren

- Als het risico acceptabel is
- Als het te kostbaar of onmogelijk is om het risico te verkleinen door de risicobeheersings- en controlesystemen.

Mitigeren

- Als de organisatie het risico kan verkleinen door processen te veranderen of de interne beheersing te verbeteren.

Overdragen

- Als er verzekeringen beschikbaar zijn die financiële verliezen compenseren
- Als samenwerken met een andere onderneming tot de mogelijkheden behoort.

Terugtrekken

- Als het risico te groot is en een bedreiging vormt voor de levensvatbaarheid van de organisatie.

Najagen

- Als meer risico voor de organisatie wenselijk is in ruil voor een hoger verwacht rendement of groei.

55 | PwC Waarde toevoegen in tijden van verandering

< <• ≡ >

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Dynamisch risicoprofiel
Elke organisatie heeft een eigen risicoprofiel, afhankelijk van bijvoorbeeld de sector, de (internationale) markten, de keten waarin wordt geopereerd en de fase van de levenscyclus waarin het bedrijf zich bevindt. Het risicoprofiel verschilt dus per bedrijf. In essentie worden alle organisaties echter geconfronteerd met universele risico's, die onvermijdelijk gepaard gaan met ondernemerschap. De mate en de aard van de dreiging zal steeds verschillen. Andere risico's zijn nieuw en komen voort uit de snel veranderende omgeving, zoals het risico van cybercrime en het toenemende reputatierisico in een onlinewereld en een dynamisch geopolitiek krachtenveld.

Het risicoprofiel van een organisatie is niet statisch, maar dynamisch: zowel de organisatie als de omgeving kan veranderen. Dat kan steeds andere en onbekende risico's meebrengen, of de impact van risico's op de bedrijfsvoering, de langetermijnwaardcreatie en zelfs de continuïteit beïnvloeden. Het agenderen van de beoordeling en bespreking van risico's ademt mee met die dynamiek.

Breed spectrum aan risico's overzien
Gedegen risicobeheersing en interne controle richt zich op een breed spectrum aan risico's:

- intern en extern
- kwantitatief en kwalitatief
- financieel en niet-financieel
- in verschillende risicocategorieën:

Waarop let een effectieve auditcommissie bij het risicoprofiel en de risicobereidheid?		
Verantwoordelijkheden van de auditcommissie	Aandachts- en vraagpunten	
Geïnformeerd worden over het risicoprofiel van de onderneming	• Beschikt het management over een gestructureerd proces om het risicoprofiel en de bijbehorende managementactiviteiten periodiek in kaart te brengen, te evalueren en hierover te rapporteren aan de auditcommissie? • Als dat het geval is, is de auditcommissie ervan overtuigd dat dit proces een compleet overzicht geeft van het risicoprofiel van de onderneming? • Worden de soorten risico's die moeten worden gemonitord en waarover het management moet rapporteren, omschreven in het reglement van de auditcommissie? Doorgaans zullen in deze lijst de volgende risico's zijn opgenomen: - risico's die gepaard gaan met het opdelen in belangrijke bedrijfsprocessen (met name de financiële verslaglegging en de financiële managementprocessen); - aan fraude gerelateerde risico's; - risico's ten aanzien van het niet voldoen aan wet- en regelgeving; - de bedrijfscontinuïteit en de mate waarin men is voorbereid op rampen; - IT-risico's (zoals cybersecurity). • Volgt het programma van de bijeenkomsten van de auditcommissie de ontwikkeling van significante risico's en de actieplannen van het management?	
Het overzicht hebben dat de mate waarin risico wordt genomen, in lijn is met de risicobereidheid van de onderneming	• Begrijpt de auditcommissie de belangrijkste componenten van het risicomanagementraamwerk van de onderneming? • Welke processen, verantwoordelijkheden en invloeden of gedragingen binnen de organisatie zijn van belang voor de manier waarop de risico's van de onderneming wordt beheerd? • Hoe verkrijgt de auditcommissie zekerheid dat deze componenten naar behoren functioneren? Wordt de uitvoering van het raamwerk geborgd door middel van kpi's? • Welke processen zijn er om te borgen dat er in de besluitvorming door het management voldoende rekening wordt gehouden met risico's en onzekerheden en hoe verkrijgt de auditcommissie zekerheid dat het management effectief opereert? • Hoe verkrijgt de auditcommissie zekerheid dat de informatie die zij krijgt, compleet, betrouwbaar en accuraat is? • Hoe vormt de auditcommissie zich een beeld over de wijze waarop de cultuur binnen de organisatie van invloed is op het beheersen van risico's en onzekerheden? • Welke informatie heeft de auditcommissie tot haar beschikking over risicovolle gebeurtenissen die hebben plaatsgevonden en die binnen haar autoriteit vallen?	

- | | | |
|--|--|---|
| <ul style="list-style-type: none">- strategie;- bedrijfsvoering/operatie (inclusief de beloningsstructuur van bestuurders en medewerkers);- financieel;- compliance (naleven van wet- en regelgeving en het voldoen aan normen | <ul style="list-style-type: none">van stakeholders/de maatschappij);- verslaggeving. | |
| | <p>■ De rol van de auditcommissie</p> <p>De auditcommissie voert een dialoog met het bestuur over de manier waarop wordt omgegaan met strategische, operationele,</p> | <p>compliance- en verslaggevingsrisico's. Naast deze hoofdcategorieën is het van belang dat de auditcommissie zicht heeft op een aantal specifieke risico's, die onderdeel kunnen zijn van verschillende categorieën.</p> |

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De Code benoemt een aantal voorbeelden van risico's die om beheersing vragen of die kunnen duiden op misstanden of onregelmatigheden. Voorbeelden van strategische, operationele, compliance en verslaggevingsrisico's zijn risico's als klimaatverandering, sociale ongelijkheid, fiscale risico's, frauderisico's, witwasrisico's en risico's van informatie- en communicatietechnologie (waaronder op het gebied van cybersecurity, leveranciers- en ketenafhankelijkheden, data protectie en risico's verbonden aan nieuwe technologieën en veranderende businessmodellen, zoals op het gebied van ethisch verantwoorde toepassing van nieuwe technologieën (bijvoorbeeld Responsible AD)).

Reputatie: risico in het kwadraat
Het reputatierisico loopt dwars door alle risicocategorieën en specifieke risico's heen en kent geen materialiteit. In feite gaat het om een risico in het kwadraat: elk strategisch, operationeel, compliance- en verslaggevingsrisico kan ook de reputatie van de organisatie negatief beïnvloeden en de schade daarvan kan een grotere impact hebben dan het initiële risico. De auditcommissie kan nagaan of het bestuur zich bewust is van het reputatierisico, dit voldoende laat meewegen in de risicoafweging en heeft geïntegreerd in de **hard** en de **soft controls**.

Hoe vaak risico's beoordelen?

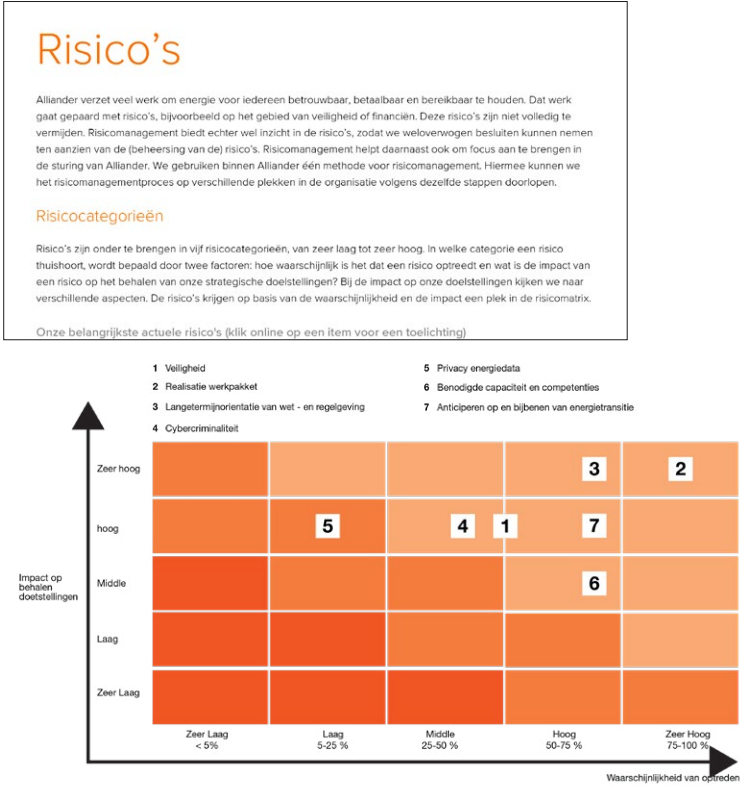
- voornaamste risico's die 'statisch' van aard zijn: één keer per jaar;
- voornaamste risico's die meer dynamisch van aard zijn: twee tot drie keer jaar of zelfs vaker.

Vragen om 'heat map'
Hoe kan de auditcommissie zorgen voor goed zicht op de voornaamste risico's en hoe deze zich in de loop van de tijd ontwikkelen? Hoe kan voorkomen worden dat bepaalde risico's (die later cruciaal kunnen blijken te zijn) zich aan de radar van het toezicht onttrekken? In de praktijk is het gebruikelijk dat het bestuur jaarlijks de voornaamste risico's bespreekt en vaststelt. De auditcommissie kan het bestuur vragen naar het opstellen van een **heat map** waarop de voornaamste risico's zijn aangegeven. De auditcommissie (en de raad van commissarissen) kan aan de hand van een **heat map** niet alleen gemakkelijker beoordelen of alle risico's voldoende beheerst en gemonitord worden, maar deze disciplineert ook het bestuur. Ook kan een **heat map** als basis dienen voor of worden opgenomen in het bestuursverslag.

'Heat map': kans versus impactrisico's
Een **heat map** geeft alle geïdentificeerde risico's weer en zet de kans dat deze risico's zich voordoen af tegen de mogelijke impact ervan. Het bestuur geeft door het periodiek opstellen van heat maps blijk van alertheid op (nieuwe) risico's

en de monitoring daarvan. De auditcommissie kan **heat maps** gebruiken voor gericht toezicht op de effectiviteit van de interne risicobeheersings- en controlesystemen: zijn ze (in)gericht op de voornaamste risico's en worden ze bijgesteld om verschuivingen in het risicoprofiel het hoofd te

bieden?
Hieronder een voorbeeld van een heat map (zie bestuursverslag Alliander 2018, winnaar FD Henri Sijthoff-prijs 2019 in de categorie niet-beurgenoteerde bedrijven):



2. Monitoren van de interne risicobeheersings- en controlesystemen

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie



Het bestuur ontwerpt, implementeert en onderhoudt adequate interne risicobeheersings- en controlesystemen en monitort de werking ervan. Het bestuur bespreekt de effectiviteit van de systemen met de auditcommissie en legt daarover verantwoording af aan de raad van commissarissen.

De rol van de auditcommissie

Het is de taak en de verantwoordelijkheid van de auditcommissie om de raad van commissarissen te ondersteunen bij de beoordeling van de effectiviteit van de interne risicobeheersings- en

controlesystemen. De auditcommissie ziet toe op de opzet en de werking van de systemen voor het eerder genoemde brede spectrum aan risico's (zowel strategisch, operationeel en financieel als op het gebied van compliance en verslaggeving) en op de jaarlijkse beoordeling daarvan door het bestuur. De auditcommissie brengt daarover verslag uit aan de raad van commissarissen.

Aansluiten bij COSO-raamwerk?

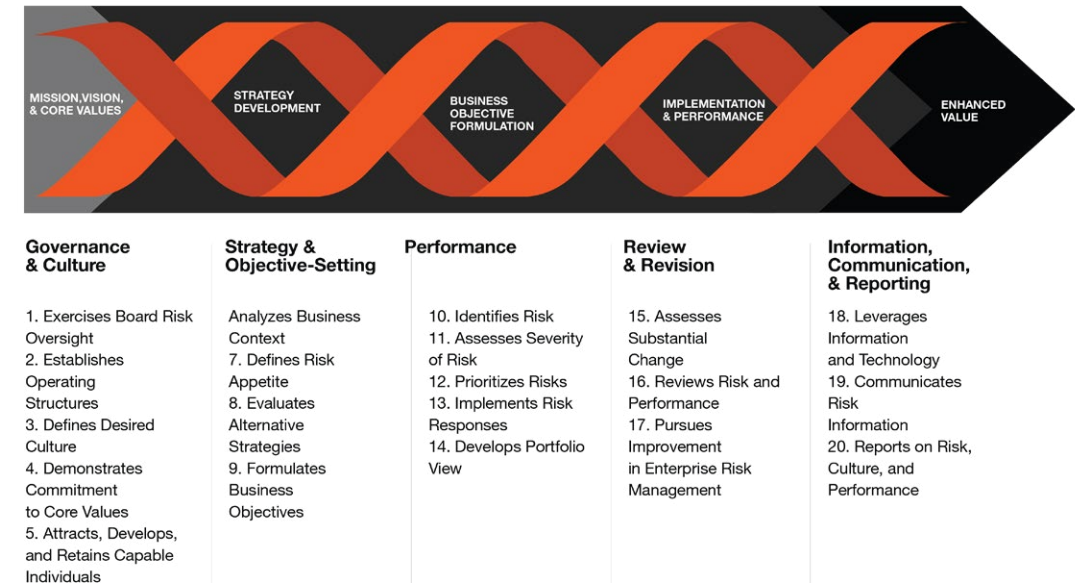
De Code geeft geen nadere richtlijnen voor de interne risicobeheersings- en controlesystemen. Wel stelt de Code dat het voor de hand ligt dat

het bestuur bij de beschrijving van de opzet en de werking van de systemen in het jaarverslag aangeeft welk raamwerk of normenkader (bijvoorbeeld het COSO-raamwerk voor interne beheersing) is gehanteerd bij de evaluatie daarvan. Dat impliceert de verwachting dat Nederlandse beursgenoteerde ondernemingen voor de inrichting en evaluatie van het organisatie-specifieke risicomanagementsysteem aansluiting zoeken bij algemeen erkende, internationaal geaccepteerde raamwerken, zoals het COSO

Integrated Internal Control Framework (2013), of COSO Enterprise Risk Management (ERM) Framework (2017). Zie [pwc.nl](https://www.pwc.nl) voor meer informatie.

Als de organisatie nog geen algemeen erkend risicoraamwerk hanteert, moet de auditcommissie onderzoeken wat de reden daarvan is en of het alternatief garant staat voor een even goede inrichting en evaluatie van de risicobeheersings- en controlesystemen. Als dit laatste niet het

COSO Enterprise Risk Management



Bron: COSO, Enterprise Risk Management - Integrating with Strategy and Performance.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

geval blijkt, moet de auditcommissie staan op aanpassing van het risicoraamwerk. Wanneer de organisatie wel een dergelijk raamwerk hanteert, kan de auditcommissie dit ook zelf als richtlijn gebruiken voor de monitoring van de risicosystemen.

Best practice

Inzet data-analyse voor risicobeheer en interne controle

De auditcommissie kan het bestuur vragen of en hoe de organisatie gebruikmaakt van (voorspellende) data-analyse voor het identificeren en managen van risico's. Het draait bij data-analyse om het samenbrengen van informatie waarover de organisatie al beschikt – zowel van interne als externe bronnen – tot waardevolle analyses. Dat kan helpen bij de beheersing en de monitoring van risico's.



Uit de praktijk

Twee voorbeelden van datagestuurd risicomanagement

- Een groothandel in consumentengoederen maakt zich zorgen over het risico dat de inkoopketen besmet wordt door namaakproducten. Deze kunnen immers leiden tot problemen op het gebied van veiligheid en kwaliteit en schade toebrengen aan merk en reputatie. Door het vergelijken van sales- en marketinggegevens met sociale media en internetactiviteit is het bedrijf in staat om de landen of regio's te identificeren waar de kans dat namaakgoederen de inkoopketen binnenkomen het grootst is. Die landen of regio's kunnen vervolgens zorgvuldiger gemonitord worden.
- Veel organisaties maken zich zorgen over de naleving van aanbestedingsregels. Voor het beheersen van dit compliancerisico kan data-analyse worden ingezet: door transacties per leverancier te linken aan de betrokken inkoopmanagers kunnen ongewenste patronen in het inkoopgedrag worden ontdekt.

Waarop let een effectieve auditcommissie bij het toezicht op de interne beheersing?

Verantwoordelijkheden van de auditcommissie	Aandachts- en vraagpunten
Inzicht hebben in de mate van interne controle binnen de organisatie	• Begrijpt de auditcommissie wat de belangrijkste bedrijfsprocessen zijn en waar strakke interne controles nodig zijn? • Ontvangt de auditcommissie betrouwbare informatie over fraude-incidenten of ernstige tekortkomingen op het gebied van control? • Verschafft het bestuur inzicht aan de auditcommissie over de effectiviteit van de interne controle van de belangrijkste bedrijfsprocessen? In hoeverre organiseert het bestuur voldoende contactmomenten om deze inzichten te ondersteunen? • Verkrijgt de auditcommissie voldoende onafhankelijke terugkoppeling aangaande de uitvoering van de belangrijkste controles door de interne auditor en de externe accountant van de organisatie? • Hoe bewaakt de auditcommissie de implementatie door het bestuur van corrigerende acties naar aanleiding van zwakke plekken binnen de interne controle?



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

- 1. Beoordelen van de risico's
- 2. Monitoren van de interne risicobeheersings- en controlesystemen**
- 3. Afstemmen met Internal Audit
- 4. Afstemmen met de externe accountant
- 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie



Risico's voor effectieve interne beheersing:

De auditcommissie vraagt het bestuur periodiek hoe wordt omgegaan met potentiële risico's voor de effectiviteit van de interne beheersing van organisaties.

Management doorbreekt beheersingsmaatregelen:

Auditcommissies moeten zorgvuldig in de gaten houden of – en hoe – het management vastgelegde beheersingsmaatregelen kan doorbreken en welke procedures die risico's kunnen verkleinen.

Externe dienstverleners:

Auditcommissies van organisaties die (een gedeelte van) belangrijke taken uitbesteden – zoals de administratie, de verwerking van informatiesystemen, de ontwikkeling van systemen of het testen van interne beheersingsmaatregelen – moeten zich ervan vergewissen dat het management deze externe dienstverleners op de juiste wijze monitort en zich ervan verzekert dat de geleverde diensten volstaan.

Informatietechnologie:

De auditcommissie moet zich ervan vergewissen dat haar leden over de kennis beschikken of hiervoor kunnen leunen op interne of externe experts, om de complexe informatietechnologie te begrijpen die ten grondslag ligt aan de interne beheersingsmaatregelen. Auditcommissies moeten in staat zijn inzichtelijke vragen te stellen over beheersingsmaatregelen met betrekking tot de integriteit van klantgegevens, privacy, beveiliging en toegang. Daarnaast kunnen nieuwe

technologieën en ontwikkelingen op gebieden als AI, sociale media en cloudcomputing zowel tot kansen als tot risico's leiden, die misschien ook door het management nog niet ten volle worden ingezien.

Fusies en overnames:

Auditcommissies moeten aan bestuurders vragen hoe zij de interne beheersingsmaatregelen van de overnamekandidaat beoordelen bij het overwegen van een dergelijke transactie. Tijdens het due-diligenceonderzoek moet er specifiek aandacht zijn voor het systeem van interne beheersingsmaatregelen en de gevolgen hiervan voor de externe rapportagevereisten – met name voor de staat van de interne-controleomgeving van de overnamekandidaat en de plannen van de organisatie om de operationele activiteiten samen te voegen en de mogelijkheid om de beheersingsmaatregelen te standaardiseren na de acquisitie.

Impact van herstructurering:

De controleomgeving kan significant veranderen door afname van het personeelsbestand, veranderingen van het bedrijfsmodel, consolidatie van de operationele activiteiten, de verkoop van activa en uit deze activiteiten resulterende veranderingen van processen en informatiesystemen. Auditcommissies moeten zich op de hoogte stellen van hoe het management de impact van zulke veranderingen op de interne controle aanpakt.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

3. Afstemmen met Internal Audit

De auditcommissie mag voor de beoordeling van de interne controle en de monitoring daarvan niet alleen afhankelijk zijn van de informatie van het bestuur. Om deze informatie in perspectief te zetten, kan de auditcommissie een beroep doen op een andere interne informatiebron: Internal Audit. Deze functie of afdeling, indien aanwezig, heeft volgens de Code expliciet tot taak om de opzet en de werking van de interne risicobeheersings- en controlesystemen te beoordelen en doet daarnaar een eigen onderzoek. De resultaten van dat onderzoek worden niet alleen gerapporteerd aan het bestuur, maar ook aan de auditcommissie (de kernpunten). Overigens is er in de praktijk niet altijd sprake van de taken en verantwoordelijkheden van een interne auditfunctie zoals bedoeld in de Code. (Zie ook hoofdstuk 6, deel I, over de relatie van de auditcommissie met Internal Audit.)

Waarover rapporteert Internal Audit?

In de onderzoeksresultaten van Internal Audit wordt in ieder geval aandacht besteed aan:

- gebreken in de effectiviteit van de interne risicobeheersings- en controlesystemen;
- bevindingen en observaties die van wezenlijke invloed zijn op het risicoprofiel van de organisatie; en
- tekortkomingen in de opvolging van de aanbevelingen van Internal Audit.

De rol van de auditcommissie

De auditcommissie keurt jaarlijks het werkplan van Internal Audit goed, evenals tussentijdse wijzigingen daarin. Aanleidingen voor bijstelling van het werkplan kunnen zijn:

- een veranderend risicoprofiel door een bijstelling van de strategie;
- een wijziging in externe omstandigheden;
- signalen uit de organisatie;
- een vermoeden van misstanden en onregelmatigheden;
- tussentijdse bevindingen van Internal Audit.

De auditcommissie kan Internal Audit ook zelf proactief vragen aandacht te besteden aan bepaalde aspecten van risicobeheer en interne controle. De auditcommissie kan Internal Audit (namens de raad van commissarissen) verder expliciet vragen om het verlenen van assurance over de opzet en de werking van (onderdelen van) de interne risicobeheersings- en controlesystemen. Gebruikelijk is dat Internal Audit rapporteert over de in het afgelopen kwartaal uitgevoerde onderzoeken. De auditcommissie kan vervolgens een dialoog aangaan met het bestuur en andere functionarissen over de onderzoeksresultaten van Internal Audit, bijvoorbeeld over geconstateerde zwakke plekken of gebreken in risicobeheer of interne controle.

(Zie verder hoofdstuk 6, deel I, over de relatie van de auditcommissie met Internal Audit.)

4. Afstemmen met de externe accountant

De auditcommissie bespreekt met de externe accountant jaarlijks de belangrijkste risico's van de jaarverslaggeving die deze heeft benoemd in het controleplan, dat wordt goedgekeurd door de auditcommissie. Daarnaast deelt de externe accountant zijn of haar bevindingen in de interim-rapportage en het accountantsverslag, onder meer ten aanzien van de interne risicobeheersings- en controlesystemen.

De externe accountant komt voor de controlewerkzaamheden in de gehele organisatie en ziet en hoort veel. De accountant kan daarnaast vergelijken met andere controleorganisaties. Daarmee is de externe accountant een waardevolle informatiebron. (Zie verder hoofdstuk 6, deel II voor de relatie van de auditcommissie met de externe accountant.).



5. Interne en externe verantwoording

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
- 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Interne rapportageketen
Voor langetermijnwaardecreatie en continuïteit is gedegen risicobeheer en in control zijn cruciaal. Dat vraagt om een uitgebreide verantwoording, zowel intern als extern. (Zie daarvoor ook hoofdstuk 9: Communicatie). De auditcommissie bespreekt tijdens haar vergaderingen regelmatig de verantwoording van het bestuur over het in control zijn en krijgt ook een rapportage van Internal Audit – indien beschikbaar – over de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen. Op haar beurt rapporteert de auditcommissie aan de raad van commissarissen.

Externe rapportage
Het bestuur rapporteert in het jaarverslag over de werking van de interne beheersing. Voor bedrijven die zich houden aan de Corporate governance code is dit specifiek gemaakt in de VOR, zie pagina 63. De auditcommissie houdt hierop toezicht, ook vanuit haar andere taak: toezien op de integriteit en de kwaliteit van de verslaglegging. De raad van commissarissen legt vervolgens verantwoording af over het uitgeoefende toezicht in het afgelopen boekjaar. Hierin kan ook verslag worden uitgebracht over het toezicht op het risicobeheer. De auditcommissie levert daarvoor input: het gaat hier immers om een van haar belangrijkste taken en verantwoordelijkheden.

Interne verantwoording van het bestuur, na bespreking in de auditcommissie, aan de raad van commissarissen
Interne rapportage van Internal Audit
Interne verantwoording door de auditcommissie aan de raad van commissarissen
Externe verantwoording door de raad van commissarissen in het verslag dat deel uitmaakt van de jaarstukken
Externe verantwoording door het bestuur in het bestuursverslag

Verklaring omtrent risicobeheersing
Volgens de Code moeten beursgenoteerde vennootschappen vanaf 1 januari 2025 de verklaring omtrent risicobeheersing (VOR) opnemen in het bestuursverslag. Met de aanpassingen in de Code moet het bestuur van de onderneming in het bestuursverslag ook verklaren dat interne risicobeheersings- en controlesystemen ten minste een beperkte mate van zekerheid geven dat de duurzaamheidsverslaglegging geen



- Tien vragen voor auditcommissies over de beoordeling van het risicoprofiel (inclusief de risicoparagraaf) in het jaarverslag**
1. Is het opgenomen risicoprofiel in het jaarverslag in overeenstemming met de informatie die eerder door het bestuur is gepresenteerd en met de auditcommissie is besproken?
 2. Voldoet het risicoprofiel aan de van toepassing zijnde wettelijke informatieverplichtingen?
 3. Zijn er toereikende informatiesystemen en interne risicobeheersings- en controlesystemen die een betrouwbare risicoverslaglegging waarborgen?
 4. Is de auditcommissie tevreden met de uitleg van het bestuur over de criteria om bepaalde risico-informatie wel en niet te verstrekken in het jaarverslag? Stelt het jaarverslag de voornaamste bedrijfs- en strategische risico's aan de orde, evenals de mogelijke gevolgen en de wijze hoe met deze risico's wordt omgegaan?
 5. Heeft het bestuur in het jaarverslag risico-informatie uit het risicoprofiel weggelaten met het oog op de concurrentie of andere bedreigingen? Zo ja, kan de auditcommissie zich vinden in het niet opnemen van die specifieke informatie?
 6. Welke feedback is ontvangen van belangrijke institutionele of andere belangrijke investeerders over de adequaatheid van de risicoverslaggeving van de organisatie?
 7. Heeft de organisatie opmerkingen ontvangen van toezichthouders over de adequaatheid van de risicoverslaggeving?
 8. Welke opmerkingen heeft de eigen juridisch adviseur gemaakt over de risicoverslaggeving en wat heeft de organisatie met deze opmerkingen gedaan?
 9. Welke eventuele opmerkingen heeft de externe accountant over de risicoverslaggeving?
 10. Is het risicoprofiel in duidelijke, eenvoudige taal geschreven?

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

6. Enkele risicocategorieën uitgelicht

In dit deel van het hoofdstuk bespreken we een aantal (actuele) risicocategorieën die van belang zijn voor de auditcommissie:

1. strategisch
2. operationeel
3. cybersecurity
4. compliance
5. fraude
6. corruptie
7. verslaggeving
8. fiscaal

1. Strategische risico's

Een brede blik is noodzakelijk bij het beoordelen van strategische risico's: welke factoren kunnen de langetermijnwaardecreatie bedreigen? PwC heeft vijf megatrends geïdentificeerd die het businessmodel, de markten, de concurrentiepositie en de supplychain onder druk zetten en die nieuwe risico's met zich meebrengen.

De veranderingen brengen overigens ook kansen met zich mee voor nieuwe businessmodellen en andere manieren voor langetermijnwaardecreatie.

Best practices voor beoordelen strategische risico's

- Vraag naar de risico's van de bestaande of nieuwe strategie: worden die goed benoemd en inzichtelijk gemaakt?
- Vraag naar alternatieven: wat als het plan niet volledig gerealiseerd wordt of als er sprake is van tegenvallers? Hoe gevoelig is de prognose hiervoor en hoe denkt het bestuur hier dan mee om te gaan?
- Vraag naast een managementcase ook om een **sensitized case**, op basis van een minder optimistisch scenario, rekening houdend met onder meer de risico's.



De rol van de auditcommissie

Als onderdeel van haar toezicht op de risicobeheersings- en controlesystemen beoordeelt de auditcommissie of het bestuur zich voldoende bewust is van de impact van de bedreigingen en de risico's die samenhangen met de bestaande of nieuwe strategie. (Zie hiervoor ook hoofdstuk 2: Continuïteit – langetermijnwaardecreatie.)

Brede context

De strategische risicobeoordeling van een organisatie vereist een brede blik die verder reikt dan de direct zakelijke belangen. Het is van belang om de impact van maatschappelijke ontwikkelingen op de 'bredere context' waarin de organisatie opereert te overwegen. De actuele Code richt zich op de volgende aspecten:

Duurzaamheid: Integratie van milieubescherming en sociale verantwoordelijkheid in alle bedrijfsactiviteiten.

Sociale en personeelsaangelegenheden: Zorg voor goed personeelsbeleid en bevordering van diversiteit en inclusie.

Ketenverantwoordelijkheid: Verantwoorde operaties binnen de gehele toeleveringsketen van de onderneming.

Respect voor mensenrechten: Eerbiediging en bevordering van mensenrechten in al het zakelijk handelen.

Corruptie en omkoping: Actieve bestrijding en preventie van corruptie en omkoping.

Technologische impact: Beoordeling van de invloed en risico's van nieuwe technologieën en veranderende businessmodellen.

Belastingbeleid: Ontwikkeling van een belastingstrategie die aansluit op de doelstelling van duurzame, lange termijn waardecreatie, inclusief het betalen van een billijk aandeel (fair share) in de landen waarin winst wordt gerealiseerd, conform internationale verwachtingen.

Deze elementen zijn van belang in het kader van strategie voor duurzame lange termijn waardecreatie, zoals genoemd in de toelichting van de Code 1.1.1. Ze ondersteunen een integrale benadering van risicomanagement en duurzame bedrijfsvoering.

Grote OOB's zijn verplicht om een niet-financiële verklaring in hun jaarverslag op te nemen over deze thema's, plus de belangrijkste risico's die daarmee gepaard gaan.

De auditcommissie kan het thema maatschappelijke verantwoordelijkheid aangrijpen voor een robuuste discussie met het bestuur over strategisch risicobeheer. De vragen die de auditcommissie daarbij kan stellen:

- Maakt het bestuur een systematische analyse van de sociaal-maatschappelijke context waarin de organisatie opereert?
- Welke kansen en bedreigingen brengt deze context mee voor de langetermijnwaardecreatie en de continuïteit?
- Sluit het beheersen van strategische risico's en het optimaliseren van kansen (nog steeds) aan op de **purpose** en de waarden van de organisatie?

(Zie hiervoor ook hoofdstuk 3: Corporate impact.)

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's
2. Monitoren van de interne risicobeheersings- en controlesystemen
3. Afstemmen met Internal Audit
4. Afstemmen met de externe accountant
5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie



2. Operationele risico's

De auditcommissie zal de blik ook richten op operationele risico's. Hoe robuust is de inrichting en werkwijze van de organisatie en het gedrag van de mensen die er werken? Is de organisatie goed bestand tegen externe problemen, incidenten of calamiteiten? Of andersom: hoe kwetsbaar is de organisatie wanneer mensen, systemen en processen falen? Oftewel: hoe groot zijn de operationele risico's door:

- het tekortschieten van medewerkers (fouten, integriteitsschendingen);
- het tekortschieten van systemen (bijvoorbeeld de uitval van ICT-systemen);
- het tekortschieten van processen (bijvoorbeeld controlemechanismen tijdens het productieproces;
- onverwachte externe gebeurtenissen (zoals een natuurramp, of een cyberaanval).

■ De rol van de auditcommissie

Operationele risico's kunnen leiden tot forse verliezen, of zelfs het voortbestaan van de organisatie bedreigen. De auditcommissie zal het bestuur dan ook goed bevragen op operationele risico's en welke maatregelen daartegenover staan.

Continuïteit: materiële risico's en onzekerheden

Bij de beoordeling van operationele risico's moet de auditcommissie gericht zijn op de materiële risico's en onzekerheden die relevant zijn voor de verwachting van de continuïteit van de organisatie, op zowel de lange als kortere termijn. In de bestuursverklaring vermeldt het bestuur de materiële risico's en onzekerheden die relevant zijn voor de verwachting van de continuïteit van de organisatie voor een periode van twaalf maanden na het opstellen van het verslag. De auditcommissie analyseert deze risico's, bespreekt ze met het bestuur en doet verslag van haar bevindingen aan de raad van commissarissen. Cruciaal daarbij is het tijdig herkennen van de signalen dat het bedrijf zich in de gevarenzone bevindt. (Zie ook hoofdstuk 2: Continuïteit – langetermijnwaardecreatie.)

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

- 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

3. Cybersecurity

In deze paragraaf komen de volgende onderwerpen aan de orde:

- 1. cybergerelateerde regelgevingen
- 2. cyberdreigingen
- 3. cyberrisicomanagement
- 4. cybercontrolemaatregelen
- 5. cyberframeworks

In een digitale wereld met toenemende risico's zoals ransomware, generatieve AI, quantum computing en geopolitieke spanningen, wordt cybersecurity steeds belangrijker voor bedrijven. Voor organisaties die vanuit Nederland wereldwijd opereren, brengt dit zowel technologische als juridische uitdagingen met zich mee. Cyberdreigingen kunnen leiden tot financiële schade, reputatieverlies en juridische kwesties. De raad van commissarissen en de auditcommissie moeten erop toezien dat de organisatie niet alleen beschermd is tegen cyberdreigingen, maar ook voldoet aan de verscherpte wet- en regelgeving op het gebied van cybersecurity.

Dit hoofdstuk biedt een overzicht van de relevante Europese wet- en regelgeving rondom cybersecurity. Daarnaast worden maatregelen besproken voor de preventie van en reactie op ransomware-aanvallen, inclusief kritieke controlemaatregelen om de cyberweerbaarheid van bedrijven te versterken.

1. Cyberregelgeving

Er is verschillende regelgeving van toepassing of in de maak die een impact heeft op controlemaatregelen die vanuit het perspectief van cybersecurity verwacht worden.

In aparte paragrafen binnen dit hoofdstuk wordt regelgeving zoals DORA, NIS2, Data Act en AI Act behandeld. Al deze vormen van regelgeving hebben impact op controlemaatregelen vanuit cyberperspectief.

Verder is er nog regelgeving als de Cyber Resilience Act (CRA), Radio Equipment Directive (RED) en de wet Weerbaarheid Kritieke Entiteiten (Wwke/CER) en natuurlijk de AVG/GDPR. Ook deze vormen van regelgeving hebben impact op de te nemen maatregelen vanuit cyberperspectief.

Als we kijken naar de belangrijkste gebieden die vanuit het perspectief van cybersecurity geregeld moeten worden, dan betreft dat:

- beveiligen van gegevens (persoonlijke gegevens alsook bedrijfsgegevens) – zowel de toegang tot gegevens als het wijzigen van gegevens;
- goede beveiligingsprocedures en maatregelen rondom digitale componenten in producten die producten die geïmporteerd, geproduceerd of gebruikt worden. worden, geproduceerd worden of gebruikt worden;
- ervoor zorgen dat controlemaatregelen worden ontwikkeld en geïntegreerd om cyberrisico's vanuit derde partijen te beperken. Denk hierbij

bijvoorbeeld aan het testen van systemen van derde partijen die voor risico's kunnen zorgen in de bedrijfsprocessen (zoals bijvoorbeeld het softwaresysteem SolarWinds heeft veroorzaakt in verschillende IT-systemen wereldwijd);

- ervoor zorgen dat cyberincidenten snelesignaleerd, gerapporteerd (ook naar de noodzakelijke externe instanties) en opgelost worden;
- ervoor zorgen dat als er wat misgaat, men voorbereid is op dit zwarte scenario (backup/recovery, crisismanagement, Business Continuity Planning, Disaster Recovery).

Best practices

- Pak de verschillende vormen van regelgeving niet een voor een aan, maar zorg voor een geïntegreerde aanpak, waarbij één controleframework wordt ontwikkeld en gehanteerd.
- Vertaal controlemaatregelen in benodigde capabilities in de cyberfunctie.
- Zorg voor een goed cyber security operating model, waarbij cybersecurity goed belegd wordt in de organisatie en er korte en directe communicatielijnen zijn met verschillende functies in de business en de rvc/auditcommissie.

2. Cyberdreigingen

In de huidige digitale wereld worden bedrijven geconfronteerd met een steeds complexer en gevaarlijker cyberdreigingslandschap. Met name toenemende geopolitieke spanningen zorgen hiervoor in bepaalde sectoren (zoals kritieke infrastructuur, de semiconductor-industrie, voedingsindustrie en farmaceutische bedrijven). Het is essentieel dat organisaties zich bewust zijn van de belangrijkste cyberdreigingen, de actoren die deze bedreigingen veroorzaken en de redenen waarom het dreigingsbeeld verergert.

Belangrijkste cyberdreigingen

- **Ransomware:** Ransomware blijft een van de grootste cyberdreigingen. Deze aanvallen versleutelen de gegevens van een organisatie en eisen losgeld voor de ontsleuteling. Een nu al veelvoorkomende methode is de multi-extortion-aanval, waarbij data niet alleen worden versleuteld, maar ook gestolen en openbaar gemaakt dreigen te worden als het losgeld niet wordt betaald.
- **DDoS-aanvallen:** Distributed Denial of Service (DDoS)-aanvallen zijn toegenomen, mede door hacktivisme en geopolitieke spanningen. Deze aanvallen leggen websites of systemen plat door ze te overspoelen met verkeer of het verstoren van netwerken/connectiviteit, wat kan leiden tot aanzienlijke verstoringen van de bedrijfsvoering.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

- **Geavanceerde phishing:** Phishing blijft een veelvoorkomende dreiging waarbij aanvallers proberen gevoelige informatie te verkrijgen door zich voor te doen als betrouwbare entiteiten. Geavanceerde phishing-aanvallen maken gebruik van gepersonaliseerde en overtuigende technieken om slachtoffers te misleiden. Het gebruik van AI voor deze aanvallen maakt deze dreiging groter.
- **Kwetsbaarheden in IoT/OT-apparaten:** Het Internet of Things (IoT) brengt nieuwe risico's met zich mee. Elk verbonden apparaat is een potentieel doelwit voor cybercriminelen en het beveiligen van deze apparaten is vaak een uitdaging. Ook operationele technologie (OT), wat gebruikt wordt in productie- en distributieprocessen is hierbij steeds meer gevoelig.
- **Supplychain-aanvallen:** Aanvallen op de toeleveringsketen zijn in opkomst. Hierbij richten aanvallers zich op zwakke schakels in de keten om toegang te krijgen tot grotere doelwitten. Dit type aanval kan destructieve gevolgen hebben voor bedrijven die afhankelijk zijn van externe leveranciers.

Cyberdreigingsactoren

- **Staatsgerelateerde actoren:** Deze hackers werken met steun van overheden en richten zich meestal op spionage en het verstoren van kritieke infrastructures. Hoewel ze vaak geen directe bedreiging vormen voor de meeste bedrijven, kunnen ze wel een risico zijn voor organisaties die

- deel uitmaken van strategische ketens.
- **Cybercriminelen:** Dit is de grootste groep dreigingsactoren, gedreven door financieel gewin. Ze gebruiken technieken zoals ransomware en phishing om geld af te persen of gevoelige informatie te verkopen.
 - **Hacktivisten:** Deze actoren voeren aanvallen uit om politieke of maatschappelijke doelen te bevorderen. DDoS-aanvallen zijn een veelgebruikte methode om hun boodschap kracht bij te zetten.
 - **Insiders:** Bedreigingen van binnenuit komen van medewerkers of andere insiders die toegang hebben tot gevoelige informatie. Deze actoren kunnen opzettelijk of onopzettelijk schade veroorzaken.

Redenen voor toename in het dreigingsbeeld

- **Geopolitieke onrust:** Geopolitieke spanningen creëren een klimaat waarin cyberaanvallen toenemen. Staten en niet-statelijke actoren maken gebruik van de onrust om aanvallen uit te voeren. Cybersecurity-aanvallen worden veel gebruikt tijdens conflicten.
- **Nieuwe technieken van hackers:** Cybercriminelen worden steeds vindingrijker en maken gebruik van geavanceerde technieken zoals AI-gestuurde oplichting en multi-extortion-aanvallen. Deze nieuwe methoden maken het moeilijker voor bedrijven om zich te verdedigen

Best practices

- Zorg voor goede capabilities die cyberdreigingen kunnen voorkomen en dat begint bij een goede cyberhygiëne, zoals:
 - netwerksegmentatie
 - access controls
 - gegevensbeveiliging
- Zorg voor goede capabilities die mogelijke cyberincidenten zo vroeg mogelijk kunnen signaleren en voorkomen.
- Zorg voor goede capabilities om incidenten zo snel mogelijk te kunnen beperken
- Zorg voor goede capabilities om een mogelijke crisis te voorkomen en als een crisis zich voordoet deze op te lossen (backup/recovery, crisismanagement, business continuity management).

- **Toename van thuiswerken:** De verschuiving naar thuiswerken heeft nieuwe kwetsbaarheden geïntroduceerd. Zwakkere thuisnetwerken en het gebruik van persoonlijke apparaten voor werkdoeleinden bieden nieuwe kansen voor aanvallers
- **Complexiteit van moderne supplychains:** De complexiteit van moderne toeleveringsketens maakt deze kwetsbaar voor aanvallen. Bedrijven moeten rigoureuze beveiligingsmaatregelen implementeren om deze risico's te beheersen
- **Toename van IoT-apparaten:** De groei van IoT-apparaten vergroot het aanvalsoppervlak voor cybercriminelen. Elk verbonden apparaat is een potentieel doelwit en het beveiligen van deze apparaten is vaak een uitdaging.

- **Connectie tussen operationele en IT-systemen:** De groei van meer geavanceerde componenten in operationele systemen en de connectie van deze systemen naar buiten toe (naar het internet of naar IT-systemen), zorgt voor een toenemende kwetsbaarheid van deze operationele systemen, wat fatale gevolgen kan hebben voor de menselijke veiligheid en de continuïteit van de bedrijfsvoering.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

- 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

3. Cyberrisicomanagement

Om effectief risicomanagement op het gebied van cybersecurity te implementeren, moet een bedrijf verschillende stappen ondernemen:

- **Risk Taxonomy definiëren:** Een risicotaxonomie biedt een gestructureerde manier om risico's te categoriseren en te beoordelen. Dit omvat het identificeren van strategische cyberrisico's en het koppelen hiervan aan een bestaand controleraamwerk zoals NIST CSF, maar ook aan het Enterprise Risk Management systeem.

- **Risicomanagement operating model definiëren:** Een Target Operating Model (TOM) voor cybersecurity moet een holistische visie bieden die de strategische doelstellingen verbindt met de operationele uitvoering. Dit model moet de rollen en verantwoordelijkheden op strategisch, tactisch en operationeel niveau duidelijk definiëren, ook ten aanzien van het managen van cyberrisico's tussen de eerste, tweede en derde lijn.

- **Processen definiëren:** Het is essentieel om processen in te richten voor beoordeling, mitigatie, monitoring en rapportage van cyberrisico's. Dit omvat het ontwikkelen van methodieken voor het bepalen van de impact en kans van cyberrisico's, maar ook hoe risico's worden geïdentificeerd.

- **Rapportages inrichten:** Regelmatige rapportages zijn cruciaal om de voortgang te monitoren en de effectiviteit van de risicomanagement strategie te evalueren. Dit helpt ook bij het voldoen aan compliance-verplichtingen en het verhogen van de transparantie binnen de organisatie.

Bij het inrichten van het operating model zijn er verschillende uitdagingen met betrekking tot de verantwoordelijkheden van de eerste, tweede en derde lijn:

- **Eerste Lijn:** Deze lijn omvat de operationele activiteiten en teams die direct verantwoordelijk zijn voor het identificeren en beheren van cyberrisico's. Een uitdaging is het waarborgen van eigenaarschap en verantwoordelijkheid binnen de afdelingen.

Best practices

1. Het bepalen van een goede cyber risk taxonomy is cruciaal. Deze taxonomie kan dan gekoppeld worden aan cybersecurity controle maatregelen, key risk indicatoren en key control performance indicatoren. Op deze manier kan goed inzicht worden verkregen in de cyber risico's en kunnen investeringen ook gericht plaatsvinden om risico's te managen
2. Het inrichten van een goed cyberrisk operating model kan best wat tijd en voor discussie zorgen. Het is echter belangrijk om dit ook zorgvuldig te doen.
3. Cyberrisico's moeten in business termen gerapporteerd worden zodat ze ook duidelijk zijn voor de RvC en audit committee. Vaak zien we nog dat deze operationeel gerapporteerd worden (zoals het aantal patches).

- **Tweede lijn:** Deze lijn kijkt strategisch naar risico's en biedt expertise, advies en kaders aan de eerste lijn. Een uitdaging is het effectief consolideren en evalueren van gegevens uit de eerste lijn en het bieden van ondersteuning bij risicobeoordelingen.

- **Derde lijn:** De interne-auditfunctie evalueert onafhankelijk de effectiviteit van de strategieën en de beleidsmaatregelen voor cyberrisicomanagement. Een uitdaging is het bieden van assurance en het direct aan de raad van bestuur rapporteren van bevindingen over cyberrisicomanagement. Dat vereist veelal technische vaardigheden.

Het is belangrijk om duidelijke communicatiekanalen en samenwerking tussen de eerste, tweede en derde lijn te waarborgen om een effectief framework voor cyberrisicomanagement te implementeren.

4. Cybercontrolemaatregelen

Er kunnen veel maatregelen worden genomen om een bedrijf te beveiligen tegen cyberrisico's, geheel afhankelijk van de kernprocessen, de infrastructuur en het dreigingsbeeld. Deze maatregelen zou elk bedrijf in ieder geval moeten nemen:

- **Sterk wachtwoordbeleid:** Sterke wachtwoorden verminderen de kans op ongeautoriseerde toegang. Gebruik van complexe wachtwoorden en regelmatige updates zijn essentieel om accounts te beschermen tegen brute force-aanvallen
- Firewalls, netwerksegmentatie en antivirussoftware: Firewalls helpen ongeautoriseerde toegang tot het netwerk te blokkeren, terwijl antivirussoftware beschermt tegen malware en andere schadelijke software. Netwerksegmentatie zorgt voor een hogere beschermingsgraad van de verschillende netwerken voor een cyberattack, omdat deze daarmee niet automatisch impact heeft op het gehele bedrijf.
- Regelmatige back-ups van gegevens: Back-ups zorgen ervoor dat gegevens kunnen worden hersteld in geval van een cyberaanval, zoals ransomware, of andere gegevensverliesincidenten.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's
2. Monitoren van de interne risicobeheersings- en controlesystemen
3. Afstemmen met Internal Audit
4. Afstemmen met de externe accountant
5. Interne en externe verantwoording
6. Enkele risicocategorieën uitgelicht
Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

- **Training van medewerkers in cybersecuritybewustzijn:** Medewerkers zijn vaak de zwakste schakel in cybersecurity. Regelmatige training helpt hen bewust te maken van bedreigingen, zoals phishing en social engineering en hoe deze te herkennen en te vermijden.

- **Beperking van toegang tot gevoelige informatie:** Door toegang tot gevoelige gegevens te beperken tot alleen diegenen die deze nodig hebben, wordt het risico op datalekken en insider threats verminderd.

- **Encryptie van gegevens:** Encryptie zorgt ervoor dat gegevens onleesbaar zijn voor onbevoegden, zelfs als ze erin slagen toegang te krijgen tot de gegevens (tenzij ze de encryptie kunnen ontsleutelen, wat ook een toenemend risico zal zijn door quantum computing).

- **Gebruik van asset tracking voor IT-apparatuur:** Het bijhouden van de status van alle IT- apparatuur helpt bij het identificeren van kwetsbaarheden en het beheren van updates en patches.

- **Periodieke beveiligingsaudits:** Regelmatige audits helpen bij het identificeren van zwakke plekken in de beveiliging op cybergebed en zorgen ervoor dat beveiligingsmaatregelen up-to-date en effectief zijn.

- **Incidentenbeheerplan:** Een goed gedefinieerd incidentenbeheerplan zorgt ervoor dat een organisatie snel en effectief kan reageren op een cyberaanval, waardoor de schade wordt beperkt.

- Cybersecurity van de supplychain:

Beveiliging van de toeleveringsketen helpt bij het voorkomen van cyberaanvallen via leveranciers en partners, die vaak zwakkere beveiligingsmaatregelen hebben.

Zero Trust is een cybersecuritymodel dat uitgaat van het principe «vertrouw niemand, verifieer altijd». Dit betekent dat geen enkele gebruiker of apparaat automatisch wordt vertrouwd, zelfs niet als ze zich binnen het netwerk bevinden. Elke toegangspoging moet worden geverifieerd, ongeacht de locatie van de gebruiker of het apparaat. Zero Trust is niet makkelijk te bewerkstelligen in een bedrijf, maar is goed voor het beleggen van controlemaatregelen voor cybersecurity om verschillende redenen:

1. **Bescherming tegen interne en externe bedreigingen:** Door elke toegangspoging te verifiëren, verkleint Zero Trust de kans op succesvolle cyberaanvallen, zowel van binnen als van buiten de organisatie.
2. **Beperking van schade:** Door netwerken op te delen in kleinere zones en geen enkele zone automatisch te vertrouwen, blijft de schade beperkt wanneer een aanval plaatsvindt.

Best practice

Voor het bepalen van controlemaatregelen is het altijd van belang om te begrijpen wat het risico is om een goede mix van maatregelen te nemen om het risico te beperken tot een acceptabel niveau.



3. **Automatisering en continue monitoring:** Zero Trust maakt gebruik van geavanceerde technologieën, zoals multifactor authenticatie (MFA), identiteits- en toegangsbeheer en continue monitoring om cyberbedreigingen snel te identificeren en erop te reageren.

4. **Naleving van cyberregelgeving:** Zero Trust helpt organisaties om te voldoen aan verschillende regelgevingseisen door strikte controle en bescherming van gevoelige gegevens.

- 1. **Commissie**
- 2. **Continuïteit**
- 3. **Corporate impact**
- 4. **Control & Compliance**
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. **Enkele risicocategorieën uitgelicht**
Bijlagen
- 5. **Cultuur en gedrag**
- 6. **Checks & Balances**
- 7. **Corporate Reporting**
- 8. **Crisis**
- 9. **Communicatie**

5. Cyberframeworks
Er zijn verschillende frameworks die gebruikt worden voor het bepalen van de controlemaatregelen die belangrijk zijn voor IT-systemen. De volgende vier frameworks voor cybersecurity van IT-omgevingen worden vaak gebruikt:

NIST CSF
Het NIST Cybersecurity Framework (CSF) is ontwikkeld door het National Institute of Standards and Technology (NIST) en biedt een gestructureerde aanpak voor het beheren en verminderen van cyberrisico's. Het framework bestaat uit vijf kernfuncties:

1. **Identificeren (Identify):** Begrijpen en beheren van cybersecurityrisico's voor systemen, mensen, activa, data en capaciteiten.
2. **Beschermen (Protect):** Ontwikkelen en implementeren van passende beveiligingsmaatregelen om kritieke infrastructuurdiensten te waarborgen.
3. **Detecteren (Detect):** Ontwikkelen en implementeren van de juiste activiteiten om een cybersecurity-incident te identificeren.
4. **Reageren (Respond):** Ontwikkelen en implementeren van de juiste activiteiten om actie te ondernemen tegen een gedetecteerde cybersecuritygebeurtenis.
5. **Herstellen (Recover):** Ontwikkelen en implementeren van de juiste activiteiten om de organisatie weerbaar te maken en van een gedetecteerd cybersecurity-incident te herstellen.

ISO/IEC270091
ISO/IEC 27001 is een internationale standaard voor informatiebeveiligingsbeheer (Information Security Management System, ISMS). Het biedt een systematische aanpak voor het beheren van gevoelige bedrijfsinformatie, zodat deze veilig blijft. De standaard omvat richtlijnen voor het vaststellen, implementeren, onderhouden en continu verbeteren van een ISMS. Een bedrijf kan ook kiezen voor certificering, maar een certificaat zegt niet of het cyberrisico laag is, het zegt wel of een ISMS goed is ingericht en de controlemaatregelen die daarin zijn vastgesteld ook zijn ingericht.

CIS Controls:
De CIS Controls zijn een set van best practices voor cybersecurity, ontwikkeld door het Center for Internet Security (CIS), gericht op het verbeteren van de cyberverdediging. De CIS Controls zijn geschikt voor kleine tot middelgrote organisaties die snel hun beveiliging willen verbeteren.

Information Security Forum (ISF) Standard of Good Practice (SoGP):
De SOGP is een uitgebreide en praktische gids voor het identificeren en beheren van informatiebeveiligingsrisico's binnen organisaties en hun toeleveringsketens. Het framework is ontworpen om organisaties te helpen bij het integreren van goede beveiligingspraktijken in hun bedrijfsprocessen, informatiebeveiligingsprogramma's, cyberrisicomanagement en

nalevingsregelingen. Een organisatie moet lid zijn van de ISD om dit te kunnen gebruiken.

Er zijn verschillende cybersecurityframeworks voor de beveiliging van operationele technologiesystemen (OT). OT wordt gebruikt in operationele en distributieprocessen en is een belangrijk onderdeel van het cybersecurityrisicomanagement.

Het **NIST SP 800-82** biedt richtlijnen voor het beveiligen van industriële controlesystemen (ICS) en andere OT-omgevingen. Het biedt een uitgebreide gids voor het beveiligen van ICS, inclusief SCADA-systemen, Distributed Control Systems (DCS) en andere controleen automatiseringssystemen die worden gebruikt in kritieke infrastructuur. Belangrijke componenten:

Best practice
Kies een framework dat bij het bedrijf en het risicoprofiel van het bedrijf past. Als er operationele technologie in productie- en distributieprocessen gebruikt wordt, dan is het ook van belang om een framework te hebben voor de beveiliging van operationele technologie, omdat deze wezenlijk andere beveiligingsmaatregelen nodig heeft dan informatietechnologie.

1. **Assetmanagement:** Identificeren en beheren van alle OT-assets binnen de organisatie.
 2. **Risk Management:** Beoordelen en beheren van risico's die verband houden met OTsystemen.
 3. **Access Control:** Implementeren van toegangscontroles om onbevoegde toegang tot OT-systemen te voorkomen.
 4. **Network Security:** Segmenteren van netwerken om de verspreiding van aanvallen te beperken en het gebruik van firewalls en intrusion detection/prevention systems (IDS/IPS).
 5. **Incident Response:** Ontwikkelen van procedures voor het detecteren, reageren op en herstellen van cyberincidenten.
 6. **Continuous Monitoring:** Continu bewaken van OT-systemen om afwijkingen en potentiële bedreigingen snel te identificeren.
 7. **Security Policies and Procedures:** Opstellen en handhaven van beveiligingsbeleid en procedures die specifiek zijn voor OTomgevingen.
- IEC 62443** is een reeks internationale normen voor de beveiliging van industriële automatiserings- en controlesystemen. Het biedt richtlijnen voor zowel fabrikanten als eindgebruikers.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
- Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

4. Europese wetgeving voor AI, cybersecurity en data: nieuwe ontwikkelingen en de impact op auditcommissies

In dit hoofdstuk komen de volgende onderwerpen aan de orde:

- 1. AI Act
- 2. Cyber – NIS2 Act en DORA
- 3. Data – Data Act

Snelle technologische ontwikkelingen

In de afgelopen decennia hebben technologische ontwikkelingen een ongeken­de snelheid bereikt, waarbij data, kunstmatige intelligentie (AI) en cybersecurity centrale thema's zijn. Deze innovaties bieden enorme kansen voor organisaties, maar brengen ook aanzienlijke uitdagingen met zich mee. Voor auditcommissies is het van cruciaal belang om deze ontwikkelingen te begrijpen en te integreren in hun toezicht- en controlemechanismen.

Kansen & risico's

Data en AI bieden organisaties de mogelijkheid om efficiënter te werken, betere beslissingen te nemen en nieuwe markten te betreden. Data en AI kunnen bijvoorbeeld helpen bij het voorspellen van markttrends, het optimaliseren van supplychains en het personaliseren van

klantinteracties. Maar deze technologieën brengen ook uitdagingen met zich mee, zoals ethische kwesties rondom privacy en bias, en de complexiteit van het implementeren en onderhouden van geavanceerde systemen.

Cyberbeveiliging is een ander cruciaal aspect dat niet over het hoofd mag worden gezien. De toename van cyberaanvallen voor verschillende redenen kan leiden tot datalekken (vertrouwelijkheidsrisico) en het aantasten van de betrouwbaarheid en beschikbaarheid van de data, wat kan leiden tot aanzienlijke financiële verliezen en reputatieschade. Het is daarom essentieel dat organisaties proactieve maatregelen nemen om hun digitale infrastructuur te beschermen.

Europese wet- en regelgeving

De Europese Commissie (EC) heeft verschillende vormen van wetgeving geïntroduceerd om om de kansen van data, AI en cybersecurity optimaal te benutten en de uitdagingen het hoofd te bieden. Dit beleid omvat maatregelen die gericht zijn op het bevorderen van digitale vaardigheden, het verbeteren van de digitale infrastructuur, en het waarborgen van een veilige en inclusieve digitale samenleving.

De Algemene Verordening Gegevensbescherming (AVG) is een van de eerste en meest bekende vorm van Europese regelgeving, die de privacy en bescherming van persoonlijke gegevens waarborgt. De EC heeft daarnaast richtlijnen en

verordeningen ontwikkeld die specifiek gericht zijn op AI, data en cyber (zie afbeelding x).

Deze wet- en regelgeving heeft als doel een evenwicht te vinden tussen innovatie en Bescherming en stelt strikte eisen aan Organisaties, om ervoor te zorgen dat zij verantwoord omgaan met data en technologie. Voor auditcommissies betekent dit dat zij niet alleen op de hoogte moeten zijn van deze wetgevingen, maar ook moeten toezien op de naleving ervan binnen hun organisaties. Daarbij is het van groot belang om bewust te zijn van de overlap tussen de verschillende wet-en regelgeving.

Integrated governance, risk en compliance

De verschillende wetgevingen die door de EC Is geïntroduceerd, heeft een aanzienlijke impact op organisaties binnen en buiten de Europese Unie (EU). Deze wetgeving is ontworpen om specifieke aspecten van de digitale economie te reguleren, maar er is vaak sprake van overlap tussen de verschillende

Definities

- AI: Artificial Intelligence (Kunstmatige Intelligentie)
- AVG: Algemeene Verordening Gegevensbescherming
- EC: Europese Commissie
- EU: Europese Unie

regels en de controlemaatregelen die nodig zijn om aan de regelgeving te voldoen. Dit betekent dat organisaties vaak aan meerdere sets van regels moeten voldoen voor dezelfde producten, diensten of systemen.

Voorbeelden van overlap in wetgeving

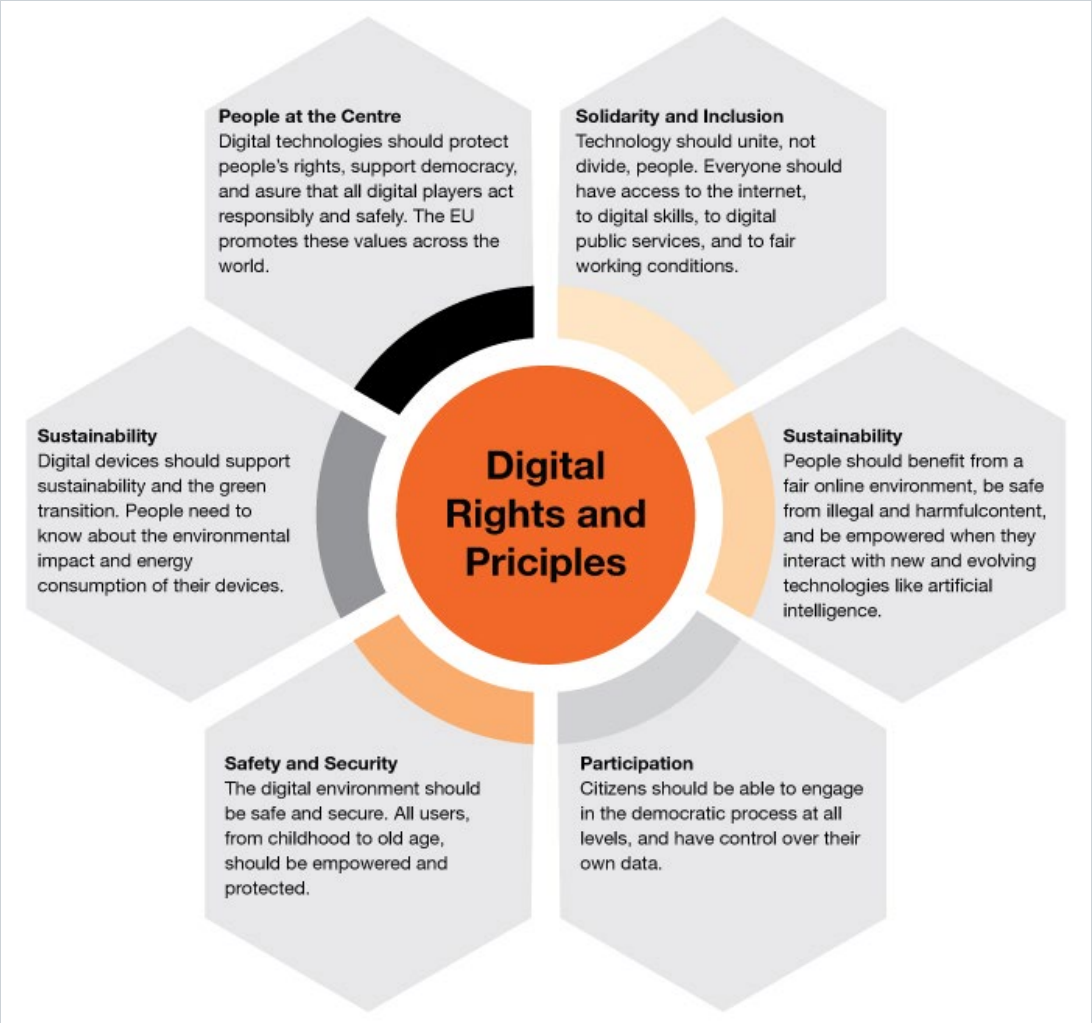
- **AI en privacy**
 - **AVG:** AI-systemen die persoonlijke gegevens verwerken, vallen onder de AVG. Dit betekent dat organisaties de privacyregels van de AVG moeten naleven.
 - **AI Act:** Daarnaast moeten AI-systemen voldoen aan de specifieke privacyregels die zijn vastgelegd in de AI Act. Dit zorgt voor een dubbele nalegingsverplichting voor organisaties die AI-technologieën gebruiken.
- **Cyberbeveiliging, data, privacy en AI**
 - **NIS2 Directive:** Deze richtlijn heeft betrekking op de beveiliging van netwerken informatiesystemen. Organisaties moeten ervoor zorgen dat hun systemen voldoen aan de beveiligingsvereisten van de NIS2-richtlijn.
 - **Data Act:** Naast de NIS2 Directive, moeten organisaties voldoen aan de regels voor data delen en beheren zoals vastgelegd in de Data Act. Dit omvat het naleven van specifieke voorschriften voor het delen en beheren van data.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

- **AVG:** Bovendien moet de AVG in acht worden genomen voor het beschermen van persoonsgegevens bij het delen van data. Dit betekent dat organisaties niet alleen moeten zorgen voor de beveiliging van hun systemen, maar ook voor de bescherming van persoonlijke gegevens.
- **AI Act:** De AI Act heeft ook gevolgen voor hoe AI-systemen en de data die deze systemen gebruiken moeten worden beveiligd.

De overlap tussen verschillende Europese wetgeving leidt ertoe dat auditcommissies een cruciale rol spelen in het waarborgen van naleving. Ze moeten erop toezien dat organisaties niet alleen voldoen aan de specifieke vereisten van elke wetgeving, maar ook dat er een geïntegreerde benadering is voor compliance en controlemaatregelen, zodat er geen sprake is van inefficiency's. Dit vereist een grondige kennis van de verschillende wetgevingen en een strategische aanpak om naleving te waarborgen zonder de operationele efficiëntie te verminderen. Dit kan uitdagend zijn, maar het biedt ook voordelen, waaronder verbeterde efficiëntie, risicobeheer, consistentie, kostenbesparing, transparantie en strategische voordelen. Door deze benadering te omarmen, kunnen auditcommissies ervoor helpen zorgen dat hun organisaties niet alleen voldoen aan de wettelijke vereisten, maar ook hun algehele prestaties en reputatie verbeteren.

De basis voor deze benadering is een geïntegreerd framework voor legal, risk, compliance en control, ondersteund door governancestructuren, processen en technologie. Op deze manier, kan het voldoen aan alle verschillende wetgeving ook resulteren in voordelen voor de bedrijfsvoering (toenemende efficiëntie in processen, betrouwbaarheid, vertrouwelijkheid en beschikbaarheid van informatie) en het vertrouwen van klanten, andere stakeholders en het ecosysteem waarin de organisatie acteert.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Deep dive

In de volgende paragrafen gaan we dieper in op de:

1. AI Act

2. Cyber – NIS2 Act en DORA

3. Data – Data Act

AI

Binnen het thema AI richten we ons op de AI Act. Deze wet stelt regels voor de en het gebruik van AI-systemen binnen de EU. Het doel van de AI Act is om de risico's van AI te beheersen en tegelijkertijd innovatie te stimuleren.

Cyber

Onder het thema Cyber bespreken we de Digital Operational Resilience Act (DORA) en de Network and Information Security (NIS) Directive. DORA richt zich op de veerkracht van de digitale operaties van financiële entiteiten, terwijl de NIS2-richtlijn de beveiliging van netwerk- en informatiesystemen binnen de EU versterkt.

Data

Het thema Data omvat de Data Act, die regels stelt voor het delen en beheeren van data binnen de EU. Deze wet is bedoeld om een eerlijke data-economie te bevorderen en de toegang tot data te verbeteren.

Hoewel we de focus leggen op de AI Act, DORA, NIS en Data Act, is het van cruciaal belang om te benadrukken dat naleving van en voorbereiding op andere relevante wetgeving eveneens noodzakelijk is. De digitale wetgeving is voortdurend in ontwikkeling, en het is essentieel om proactief te blijven en voorbereid te zijn op toekomstige veranderingen en vereisten.

Thema's

Iedere paragraaf is opgebouwd rondom dezelfde thema's:

• inleiding op de specifieke wetgeving: een overzicht van de wetgeving die in het hoofdstuk wordt behandeld;

• impact op visie en governance: Een analyse van hoe de wetgeving de strategische visie en governance van de organisatie beïnvloedt;

• inventarisatie van verschillende vereisten: Een uiteenzetting van de vereisten die voortvloeien uit de wetgeving;

• gereedstelling: voorbereiding en implementatie van de vereisten.

In iedere paragraaf zullen relevante vragen, acties en inzichten voor de auditcommissie worden gedeeld.

Cybersecurity Act (June 21)

Versterkt het EU-agentschap voor cyberveiligheid (ENISA) en stelt een kader voor cyberveiligheidscertificering in.

Digital Services Act (Aug 23)

Regulering van online platforms, aanbevelings-systemen en gerichte reclame

NIS2 Directive (Oct 24)

Beheer van cyberbeveiligingsrisico's door essentiële entiteiten (nutsbedrijven, infrastructuur, overheidsadministratie) en belangrijke entiteiten (voeding, productie, digitale aanbieders)

Data Act (Sept 25)

Delen van niet-persoonlijke gegevens die zijn gegenereerd door IoT- en cloudapparaten en -services

The AI Act (Aug 26)**

Eisen voor de veiligheid, gezondheid, elektromagnetische compatibiliteit en efficiënt gebruik van het radiospectrum voor radioapparatuur

ePrivacy Regulation (draft)***

Zorgt voor cyberbeveiliging van producten met digitale elementen, zoals hardware en software

2018

General Data Protection Regulation (May 18)

Zorgt voor cyberbeveiliging van producten met digitale elementen, zoals hardware en software

2021

Digital Markets Act (May 23)

Zorgt voor cyberbeveiliging van producten met digitale elementen, zoals hardware en software

2023

Data Governance Act (Sept 23)

Delen en hergebruik van beschermde gegevens in het bezit van de publieke sector en voor data-altruïsme

2024

Digital Operational Resilience Act (Jan 25)*

Versterkt de IT-beveiliging van financiële instellingen zoals banken, verzekeringsmaatschappijen en beleggingsondernemingen

2025

Radio Equipment Directive (Aug 25)*

Eisen voor de veiligheid, gezondheid, elektromagnetische compatibiliteit en efficiënt gebruik van het radiospectrum voor radioapparatuur

2026

Cyber Resilience Act (Dec 27)

Zorgt voor cyberbeveiliging van producten met digitale elementen, zoals hardware en software

2027

AI Liability Directive (draft)

Eisen voor de veiligheid, gezondheid, elektromagnetische compatibiliteit en efficiënt gebruik van het radiospectrum voor radioapparatuur

Unknown

73 | PwC Waarde toevoegen in tijden van verandering

<

<.

≡

>

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

NIS2

De Wet beveiliging netwerk- en informatie-systemen (Wbni) is de Nederlandse implementatie van de Europese Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn). De Wbni trad in werking op 9 november 2018. De Wbni is van toepassing op aanbieders van essentiële diensten en digitale dienstverleners. Essentiële diensten zijn diensten die van cruciaal belang zijn voor de instandhouding van kritieke maatschappelijke en economische activiteiten. Voorbeelden hiervan zijn energie, water, transport en gezondheidszorg. Digitale dienstverleners omvatten aanbieders van online marktplaatsen, online zoekmachines en cloudcomputerdiensten.

De NIS2-richtlijn, die op 16 januari 2023 in werking is getreden, markeert een belangrijke stap in de verbetering van de digitale veiligheid binnen de EU. De NIS2-richtlijn breidt het toepassingsgebied uit naar meer sectoren en introduceert strengere beveiligingsvereisten en snellere incidentrapportage. De belangrijkste wijzigingen zijn:

- **uitbreiding van sectoren:** naast de sectoren die al onder de oorspronkelijke NIS-richtlijn vielen, zijn sectoren zoals de voedingsmiddelenindustrie, de chemische industrie en de ruimtevaart toegevoegd;
- **strengere beveiligingsvereisten:** bedrijven moeten nu voldoen aan hogere beveiligingsnormen, waaronder het implementeren van passende technische en

organisatorische maatregelen om risico's te beheersen;

- **snellere incidentrapportage:** bedrijven moeten incidenten sneller rapporteren aan de bevoegde autoriteiten. Dit omvat een eerste melding binnen 24 uur, een gedetailleerde melding binnen 72 uur en een eindverslag binnen een maand;
- **aansprakelijkheid van bestuurders:** bestuurders kunnen persoonlijk aansprakelijk worden gehouden voor het niet naleven van de NIS2-richtlijn. Dit betekent dat zij verantwoordelijk zijn voor het goedkeuren van risicobeheersmaatregelen en het volgen van cybersecuritytrainingen.

Deze wijzigingen zijn bedoeld om de digitale weerbaarheid van bedrijven en organisaties binnen de Europese Unie te verbeteren en een hoger niveau van informatiebeveiliging en cyberveiligheid te waarborgen.

De NIS2-richtlijn maakt onderscheid tussen ‘essentiële entiteiten’ en ‘belangrijke entiteiten’ (zie tabel). Het belangrijkste verschil tussen de twee is dat belangrijke entiteiten lagere financiële sancties zullen krijgen en onderworpen zijn aan reactief toezicht van autoriteiten. Proactief toezicht is voorbehouden aan essentiële entiteiten. Dit betekent dat een belangrijke organisatie niet te maken krijgt met direct toezicht van regelgevers en autoriteiten, tenzij er een reden voor is. Denk aan een cyberincident of een rapport van externe organisaties, zoals

auditors of andere partijen in de supplychain. De reikwijdte van sectoren is uitgebreid aangezien de Europese Commissie alle organisaties wil bestrijken die belangrijke functies in de samenleving vervullen. Dit betekent dat NIS2 ook van toepassing is op sectoren als voedselproductie, afvalbeheer en de gehele toeleveringsketen.

Tijdslijnen NIS2

De NIS2-richtlijn werd formeel aangenomen door het Europees Parlement op 28 november 2022. De implementatie van de NIS2-richtlijn in Nederland is vertraagd (update december 2024). De NIS2-richtlijn, samen met de CER-richtlijn, is sinds 17 oktober 2024 van kracht in de Europese Unie. In Nederland worden deze richtlijnen omgezet in de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke). De verwachting is dat deze nationale wetten in het derde kwartaal van 2025 in werking treden. Tot die tijd hoeven organisaties zich nog niet aan de verplichtingen uit de richtlijnen te houden, maar hebben ze wel bepaalde rechten, zoals bijstand bij cyberincidenten door een Computer Security Incident Response Team (CSIRT)



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

NIS2: Essentiële en belangrijke sectoren	
Energie - levering, distributie, transmissie en verkoop van elektriciteit, gas, olie, verwarming/koeling, waterstof, exploitanten van EV-oplaadpunten	Essentieel
Transport via lucht, spoor, weg en water (inclusief rederijen en havenfaciliteiten)	Essentieel
Bankieren/financiën – krediet, handel, markt en infrastructuur	Essentieel
Gezondheid - zorgverleners, onderzoekslaboratoria, farmaceutica, productie van medische hulpmiddelen	Essentieel
Water - drinkwaterleveranciers en afvalwaterbeheerders	Essentieel
Digitale infrastructuur en IT-diensten - DNS, naamregisters, vertrouwensdiensten, datacenters, cloud computing, elektronische communicatiediensten, beheerde diensten en beheerde veiligheidsdiensten	Essentieel
Openbaar bestuur - (centraal, regio's + lokaal optioneel)	Essentieel
Space - exploitanten van infrastructuur op de grond	Essentieel
Post- en koeriersdiensten aanbieders	Belangrijk
Afvalbeheer	Belangrijk
Chemische producten - productie en distributie	Belangrijk
Voedsel - distributie en productie	Belangrijk
Fabrikanten: medische/diagnostische apparaten, computers, elektronica, optica, machines, motorvoertuigen, aanhangwagens, opleggers, andere transportmiddelen	Belangrijk
Digitale aanbieders - online marktplaatsen, zoekmachines, sociale platforms	Belangrijk
Onderzoeksorganisaties	Belangrijk

Boetes in verband met niet-naleving van de NIS2
Voor niet-naleving van de NIS2-richtlijn kunnen bedrijven aanzienlijke boetes krijgen. Voor essentiële entiteiten kunnen de boetes oplopen tot €10 miljoen of 2% van de jaarlijkse wereldwijde omzet, afhankelijk van welk bedrag hoger is. Voor belangrijke entiteiten zijn de boetes maximaal €7 miljoen of 1,4% van de jaarlijkse wereldwijde omzet.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

DORA

DORA is een EU-regelgeving die op 16 januari 2023 in werking is getreden en vanaf 17 januari 2025 van toepassing is. Het doel van DORA is om de digitale operationele veerkracht van de financiële sector te versterken door harmonisatie van de regels met betrekking tot ICT-beveiliging. De regelgeving is van toepassing op 21 verschillende soorten financiële entiteiten, waaronder kredietinstellingen, beurzen, clearinghuizen, alternatieve fondsbeheerders, verzekeringsmaatschappijen, betalingsinstellingen, en aanbieders van cryptodiensten.

- Belangrijkste eisen voor bedrijven**
- 1. **ICT-risicobeheer:** bedrijven moeten een kader opzetten voor het beheer van ICT-risico's, inclusief risicobeoordeling en -beperking;
 - 2. **beheer van ICT-derdepartijrisico's:** bedrijven moeten maatregelen nemen om risico's van ICT-dienstverleners te beheersen, inclusief contractuele bepalingen;
 - 3. **digitale operationele veerkracht testen:** bedrijven moeten een programma voor operationele veerkrachttesten opzetten, inclusief geavanceerde tests;
 - 4. **beheer van ICT-gerelateerde incidenten:** bedrijven moeten ICT-gerelateerde incidenten beheren en belangrijke incidenten melden aan de bevoegde autoriteiten;
 - 5. **informatie-uitwisseling:** bedrijven moeten informatie en inlichtingen over cyberdreigingen uitwisselen.

- Belangrijkste uitdagingen voor bedrijven
- 1. **complexiteit van naleving:** het opzetten van een robuust ICT-risicobeheer en veerkracht testprogramma kan complex en tijdrovend zijn;
 - 2. **beheer van derde partijen:** het waarborgen van naleving door derde partijen kan een uitdaging zijn, vooral voor bedrijven die afhankelijk zijn van meerdere ICT dienstverleners;
 - 3. **kosten:** de implementatie van de vereiste maatregelen kan aanzienlijke kosten met zich meebrengen.

“DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats.”

- Council of EU

Tijdslijnen DORA

DORA trad in werking op 16 januari 2023 en is vanaf 17 januari 2025 van toepassing. Nederlandse bedrijven moeten vanaf deze datum aan de eisen voldoen.

Digital operational resilience is the ability of a financial entity to maintain and review its operational integrity and reliability, ensuring the security of its network and information systems, even during disruptions. This includes using ICT services from third-party providers to support continuous financial services and regulatory compliance.

Boetes in verband met niet-naleving van de DORA

Bedrijven die niet voldoen aan DORA kunnen aansprakelijk worden gehouden voor het niet naleven van de regelgeving. De specifieke boetes en sancties zijn afhankelijk van de ernst van de overtreding en de nationale implementatie van de regelgeving, maar kunnen oplopen tot 1% van de jaaromzet.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

EU Artificial Intelligence Act

In de snel evoluerende wereld van Artificial Intelligence (AI) speelt de auditcommissie een essentiële rol bij het toezien op een maatschappelijk verantwoorde toepassing door organisaties. Met de inwerkingtreding van de EU AI Act, medio 2024, is deze verantwoordelijkheid dagelijkse realiteit geworden. Auditcommissies moeten zich bewust zijn van de implicaties van de AI Act en van hun rol in het toezicht houden op de naleving ervan.

AI zal de komende jaren een bepalende technologie en aanjager zijn van grootschalige digitale transformatie in publieke en private sectoren en organisaties. De verwachting is dat AI rond 2030 een integraal onderdeel zal zijn van alle processen en producten in de gehele Europese waardeketen.

Voor het realiseren van de maatschappelijke en economische voordelen van AI, is vertrouwen in de rechtmatigheid, rechtvaardigheid, betrouwbaarheid en beveiliging van de systemen onontbeerlijk gebleken. Eindgebruikers van AI-systemen, stakeholders van organisaties die AI-systemen gebruiken en besluitvormers hebben zekerheid en vertrouwen nodig in AI-systemen en de wijze waarop deze worden ingezet.

Europese AI-wetgeving

Om aan deze behoefte te voldoen heeft de Europese Unie de afgelopen jaren geharmoniseerde regelgeving uitgewerkt. Deze regelgeving, beter bekend als de ‘EU AI Act’, heeft tot doel de inzet van hoogwaardige en mensgerichte AI-systemen te bevorderen en tegelijkertijd een hoog niveau van bescherming te bieden voor de gezondheid, veiligheid en fundamentele rechten van EU-burgers. De AI Act doet dat door een uitgebreid juridisch kader vast te stellen voor het ontwikkelen, aanbieden en het gebruik van AI in de interne EU-markt, in overeenstemming met de EU-waarden. De wet is van toepassing op organisaties die AI-systemen ontwikkelen, importeren, distribueren en in gebruik hebben binnen de EU-markt, ongeacht de sector en ongeacht waar ter wereld bedrijven gevestigd zijn.

De AI Act is op 1 augustus 2024 in werking getreden en de vereisten van de regelgeving worden gefaseerd van kracht in de

daaropvolgende twee tot drie jaar. De eerste vereisten, gericht op AI-systemen met een onaanvaardbaar risico, alsook de vereisten met betrekking tot de vaardigheden van AI-eindgebruikers (waaronder werknemers), zijn per 2 februari 2025 ingegaan.

De AI Act benadrukt het belang van maatschappelijk verantwoorde AI-inzet **by design**. Dat betekent dat organisaties het algehele beheer van AI-systemen op een dusdanige manier dienen in te richten dat de rechtmatigheid, rechtvaardigheid, betrouwbaarheid en beveiliging van die systemen gewaarborgd blijft gedurende de gehele levenscyclus. Een effectieve AI-governance en competentie-overstijgende operationale werkprocessen vormen daarvoor belangrijke bouwstenen. Het niet naleven van de wet kan leiden tot boetes op grond van de AI Act zelf, maar ook op grond van de Algemene Verordening Gegevensbescherming (AVG) en sectorspecifieke regelgeving. Bovendien kunnen organisaties te maken krijgen met aansprakelijkheidsclaims als ze een deficiënt AI-systeem gebruiken.

Definitie van een AI-systeem in de EU AI Act

Een AI-systeem is: “Een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen [en dat] voor expliciete of impliciete doelstellingen uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.”

Boetes voor niet-naleving van de EU AI Act

Het niet naleven van de EU AI Act kan leiden tot aanzienlijke boetes, afhankelijk van de ernst van de overtreding en de risico-classificatie van het systeem (zie ‘Risicogebaseerde classificatie, governance vereisten en verplichtingen ten aanzien van AI-systemen’ op pagina 78):

- Het inzetten van AI-systemen die als onaanvaardbaar risico worden beschouwd, kan resulteren in boetes tot €35 miljoen, of 7% van de wereldwijde jaaromzet, afhankelijk van welk bedrag hoger is.
- Het niet voldoen aan de verplichtingen voor hoogrisico AI-systemen kan leiden tot boetes tot €15 miljoen of 3% van de wereldwijde jaaromzet.
- Voor minder ernstige overtredingen, zoals het verstrekken van misleidende informatie, kunnen boetes oplopen tot €7,5 miljoen, of 1% van de wereldwijde jaaromzet.



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Risicogebaseerde classificatie, governancevereisten en verplichtingen ten aanzien van AI-systemen

Risicogebaseerde classificatie
De EU AI Act deelt AI-systemen in vier categorieën in op basis van hun potentiële risico's: onaanvaardbaar risico, hoog risico, beperkt risico en minimaal risico. Daarnaast is er in de AI Act een specifieke categorie gewijd aan General Purpose AI-systemen. Elke van voornoemde categorieën brengt eigen wettelijke vereisten met zich mee waaraan voldaan dient te worden. De verantwoordelijkheid voor het voldoen aan die vereisten varieert met de rol die een organisatie ten opzichte van een AI-systeem in kwestie heeft (ontwikkelaar, importeur, distributeur of gebruiker).

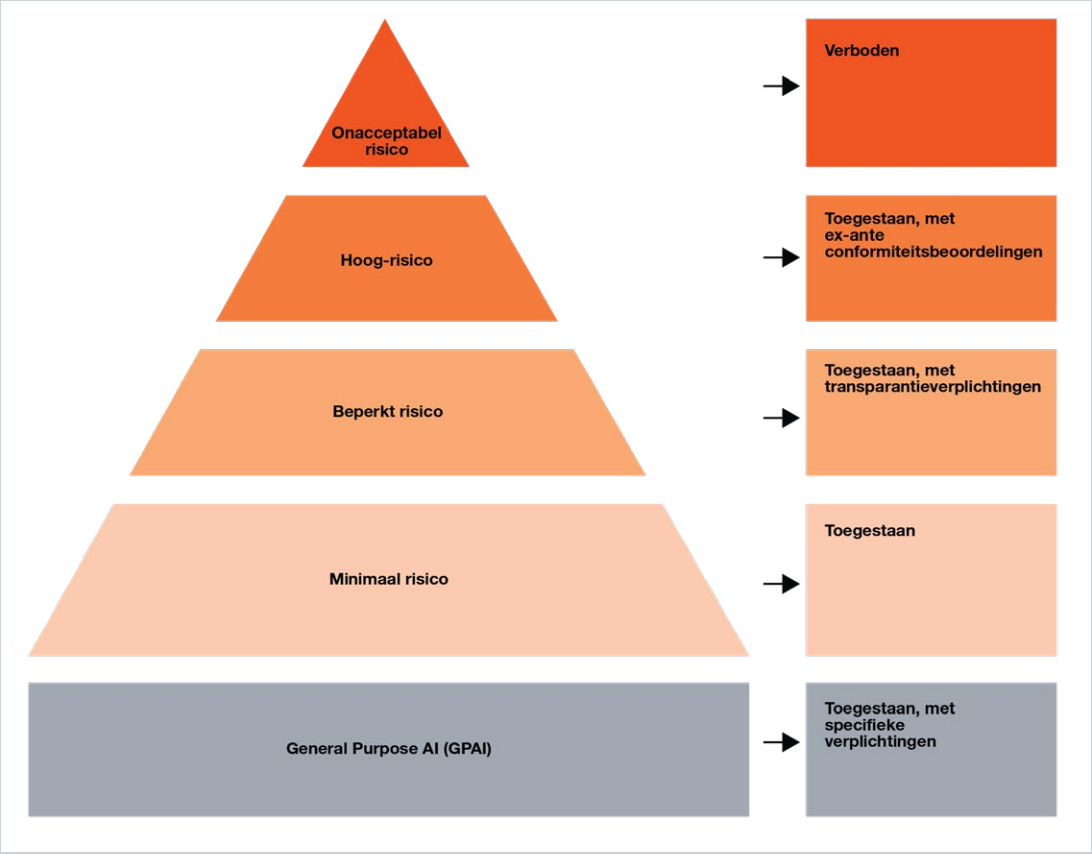
Governancevereisten en verplichtingen
AI-toepassingen die als onacceptabel risico worden geclassificeerd zijn per 2 februari 2025 verboden. AI-systemen met een hoog risico zijn toegestaan, mits voldaan wordt aan een reeks organisatorische, technisch-inhoudelijke en documentatievereisten (zie Vereisten voor hoog-risicosystemen). Voor AI-systemen met beperkt risico gelden transparantievereisten. Dat houdt in dat aanbieders van AI-systemen die rechtstreeks interacteren met natuurlijke personen, hun AI-systemen dusdanig dienen te ontwerpen en te ontwikkelen dat gegarandeerd wordt dat

individuele gebruikers zich ervan bewust zijn dat ze te maken hebben met een machine of machine-gegenereerde inhoud.

AI-systemen met minimaal risico kunnen zonder additionele vereisten in gebruik of op de markt gebracht worden. Voor het aanbieden van General Purpose AI-systemen in de interne EU-markt gelden specifieke organisatorische, technisch-inhoudelijke en documentatievereisten (onder meer opstellen van transparantie-informatie, modelvalidatie, incidentrapportage en naleving EU-copyrightregelgeving).

Inzicht in AI-toepassingen als basis voor risicoclassificatie
Om de impact van de EU AI Act op de activiteiten van een organisatie te bepalen, is allereerst inzicht nodig in bestaande (in ontwikkeling, aanschaf of gebruik zijnde) AI-toepassingen. Deze AI-inventarisatie moet minstens de volgende informatie bevatten:

- het doel en het beoogde gebruik van elk AI-systeem;
- de data die het systeem verzamelt, verwerkt, produceert en bewaart;
- de kernfunctionaliteit/werking van het systeem;
- de processen, functies en (in)directe belanghebbenden die het AI-systeem beïnvloedt.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Ook organisatie-applicaties die een AI-component hebben dienen in de AI-inventarisatie meegenomen te worden. Dit betreft bijvoorbeeld bedrijfsapplicaties die gebruikmaken van een onderliggend AI-model, zoals Chat GPT.

Deze AI-inventarisatie vormt vervolgens de basis voor de risicogebaseerde classificatie van AI-systemen onder de AI Act, zoals beschreven en het in kaart brengen van de specifieke wettelijke vereisten waaraan de betreffende organisatie dient te voldoen.

AI-systemen met een onaanvaardbaar risico:

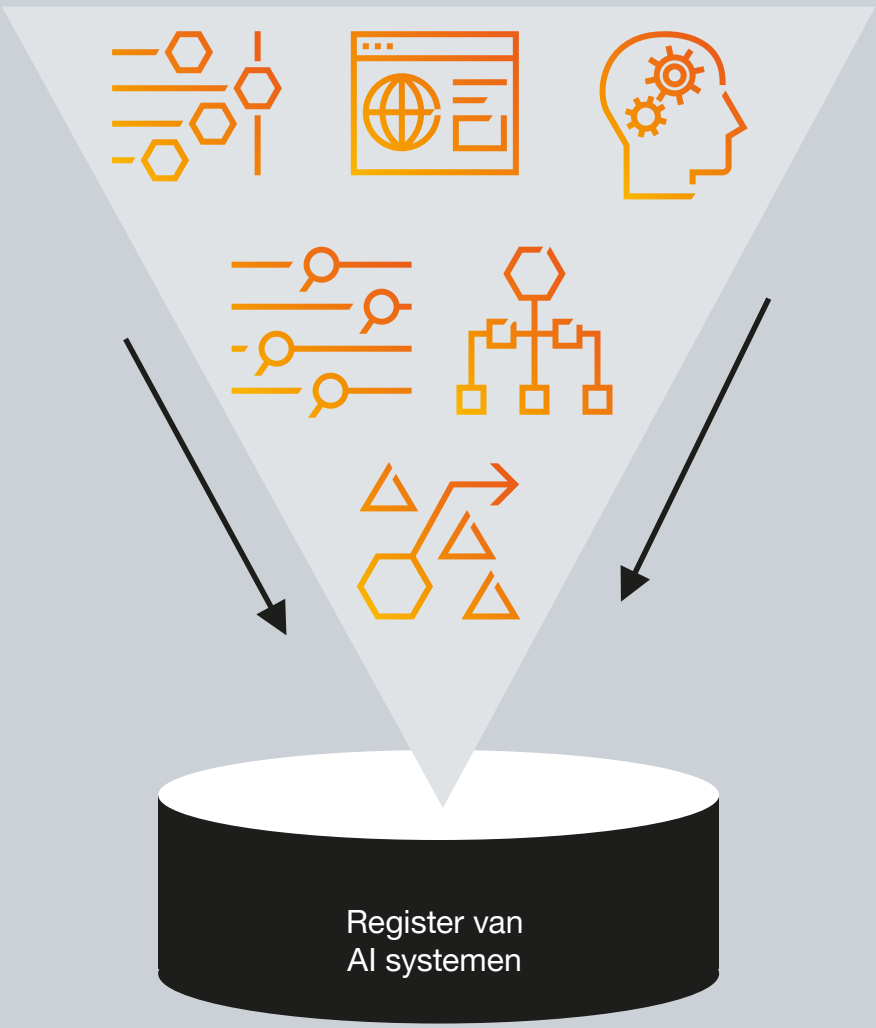
- biometrische categorisatiesystemen die gevoelige kenmerken registreren zoals ras, politieke opvattingen, lidmaatschap van een vakbond, religieuze of filosofische overtuigingen, seksuele geaardheid, behalve bij het labelen of filteren van rechtmatig verkregen biometrische gegevenssets of wanneer wetshandhavingsinstanties biometrische gegevens categoriseren;
- sociale scoring, het evalueren of classificeren van individuen of groepen op basis van sociaal gedrag of persoonlijke kenmerken, waardoor een nadelige of ongunstige behandeling van die mensen ontstaat;
- het registreren van emoties op de werkplek of in onderwijsinstellingen, behalve om medische of veiligheidsredenen.

AI-systemen met een hoog risico:

- verwijzing naar «Vereisten voor hoog-risico systemen.»

AI-systemen met een beperkt risico:

- chatbots;
- deepfakes;
- spamfilters.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Vereisten voor AI-systemen met hoog risico

Classificatie hoog-risico systeem onder de AI Act

Vanuit de eerder omschreven inventarisatie en classificatie van AI-systemen kan blijken dat een organisatie een of meerdere AI-systemen met hoog risico in ontwikkeling, aanschaf of gebruik heeft. Afhankelijk van het doel en het beoogde gebruik van deze systemen vallen ze onder Annex I of Annex III van de AI Act:

1. Annex I AI-systemen met hoog risico zijn systemen die (a) als veiligheidscomponent zijn ingebed in producten die onder de bestaande productwetgeving vallen of (b) zelf dergelijke producten vormen.
2. Annex II AI-systemen met hoog risico zijn systemen die bedoeld zijn om te worden gebruikt voor een scenario met een hoog risico, vermeld in Annex III van de AI Act.

Aanbieders van AI-systemen met hoog risico moeten aan de volgende vereisten voldoen:

1. opzetten van een risicomanagement-systeem gedurende de gehele levenscyclus van AI-systemen met hoog risico;
2. invoeren en beheren van van datagovernance en ervoor zorgen dat datasets voor training, validatie en testen relevant, voldoende representatief en, voor zover mogelijk, vrij van fouten en volledig zijn, in lijn met het beoogde doel;
3. opstellen van technische documentatie om naleving aan te tonen en autoriteiten de

informatie te verstrekken om die naleving te beoordelen;

4. ontwerpen van AI-systemen met hoog risico voor het bijhouden van gegevens, zodat het geautomatiseerd gebeurtenissen kan registreren die relevant zijn voor het identificeren van risico's op nationaal niveau en substantiële wijzigingen gedurende de levenscyclus van het systeem.
5. verstrekken van gebruiksinstructies aan partijen die AI-systemen met hoog risico downstream implementeren om naleving mogelijk te maken;
6. ontwerpen van AI-systemen met hoog risico zodat partijen die het systeem downstream implementeren menselijk toezicht kunnen toepassen;
7. ontwerpen van AI-systemen met hoog risico om de juiste niveaus van nauwkeurigheid, robuustheid en cyberbeveiliging te bereiken;
8. opzetten van een kwaliteitsmanagement-systeem om naleving van de vereisten van de AI Act te garanderen.

Pre-market conformiteitsbeoordeling

AI-systemen met een hoog risico mogen alleen op de interne EU-markt actief zijn als ze zijn onderworpen aan een pre-market conformiteitsbeoordeling. Zodra AI-systemen met hoog risico conformiteit met de AI Act hebben aangetoond, krijgt het een gestandaardiseerde CE-markering, waarna het vrijelijk kan worden ingezet op de EU-markt.

Tegenwoordig worden veel AI-systemen met een hoog risico al onderworpen aan conformiteitsbeoordelingen onder bestaande productveiligheidswetgeving. In deze gevallen zullen de eisen uit de AI Act worden geïntegreerd in de bestaande sectorale veiligheidswetgeving om dubbele administratieve lasten te voorkomen. AI-systemen met hoog risico die niet in deze categorie vallen, worden echter op zichzelf staande systemen genoemd. Deze systemen hebben twee opties voor het uitvoeren van conformiteitsbeoordelingen vóór het op de markt brengen:

- ze kunnen interne conformiteitsbeoordelingen uitvoeren, wat gelijkwaardig is aan het uitvoeren van een interne audit; of
- ze kunnen een externe auditor inschakelen die een beoordeling van het AI-systeem of -product uitvoert voordat het naar verwachting op de Europese markt komt.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

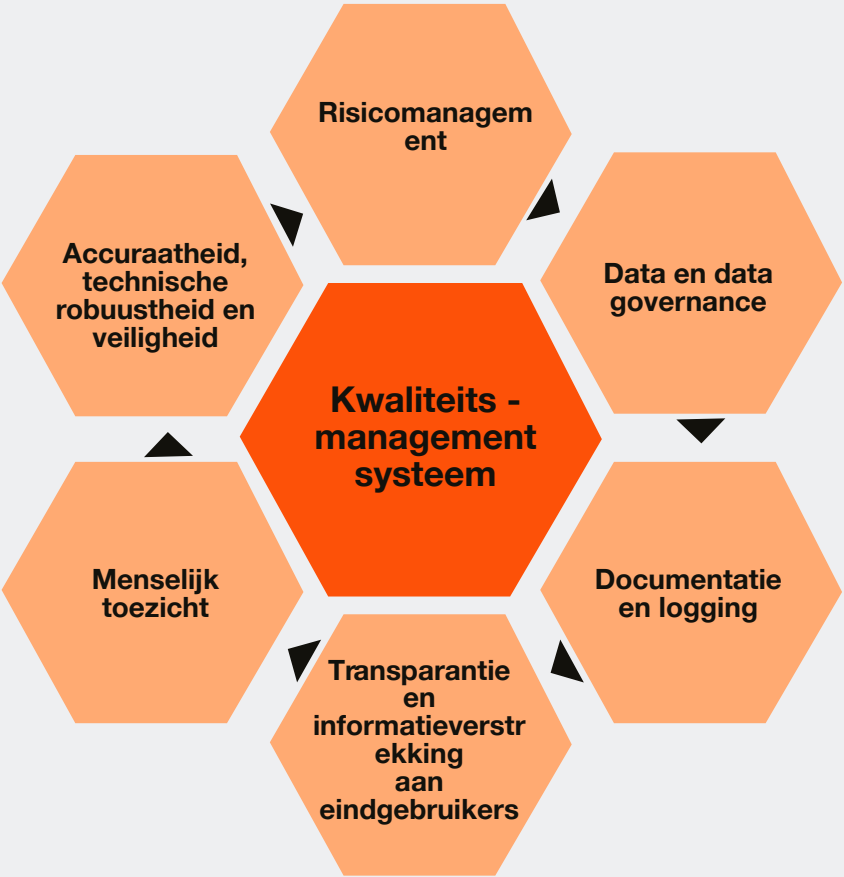
Toepassingsdomeinen AI-systemen met een hoog risico (Annex I)

Een breed scala aan gebieden, waaronder machines, speelgoedveiligheid, pleziervaartuigen, liften, apparatuur voor potentieel explosieve atmosferen, radioapparatuur, drukapparatuur, kabelbaaninstallaties, persoonlijke beschermingsmiddelen, apparaten die gasvormige brandstoffen verbranden, medische apparatuur, beveiliging van de burgerluchtvaart, twee- of driewielige voertuigen, land- en bosbouwvoertuigen, uitrusting van zeeschepen, spoorwegsysteem, motorvoertuigen en aanhangwagens daarvan en vliegtuigen.

Toepassingsdomeinen AI-systemen met een hoog risico (Annex III)

- biometrische systemen;
- veiligheidscomponenten bij het beheer en de exploitatie van kritische digitale infrastructuur, het wegverkeer en de levering van water, gas, warmte en elektriciteit;
- onderwijs en beroepsopleiding;
- werkgelegenheid, werknemersbeheer en toegang tot zelfstandig ondernemerschap;
- toegang tot en gebruik van essentiële publieke en private diensten (waaronder financiering, verzekeringen);
- wetshandhaving;
- migratie, asiel en grensbewaking;
- democratische processen en politieke campagnes.

Vereisten voor hoog-risico AI-systemen



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

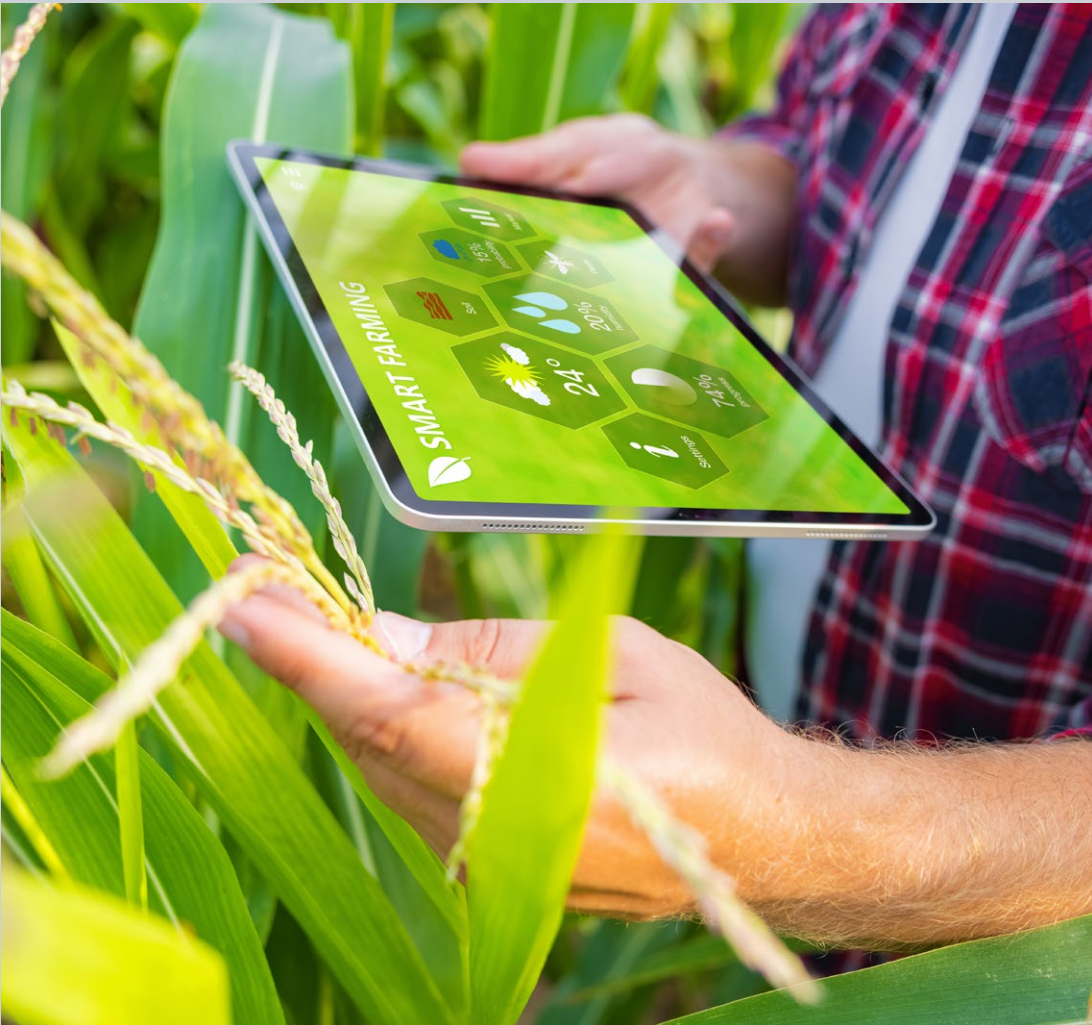
Vereisten voor hoog-risico AI-systemen (vervolg)

Post-market monitoring

Naast de conformiteitsbeoordelingen vóór het op de markt brengen, wordt van aanbieders van AI-systemen met een hoog risico ook verwacht dat zij monitoringsystemen na het op de markt brengen opzetten en documenteren. De taak van **post-market** monitoring is het documenteren en analyseren van het gedrag en de prestaties van een AI-systeem met een hoog risico na de implementatie ervan en gedurende de gehele looptijd ervan.

Beoordelingen na het op de markt brengen vormen een aanvulling op de CE-certificeringen vóór het op de markt brengen, aangezien van aanbieders van AI-systemen met een hoog risico wordt verwacht dat zij rapporteren over elk ernstig incident of defect dat een inbreuk op de EU-wetgeving vormt. Met **post-market** monitoring wordt beoogd ervoor te zorgen dat aanbieders onmiddellijk corrigerende maatregelen nemen om een AI-systeem conform te maken of volledig uit de markt te halen.

Om systeemfouten op effectieve en systematische wijze op te sporen, te rapporteren en aan te pakken, moeten aanbieders monitoringplannen na het op de markt brengen opstellen waarin rekening wordt gehouden met de beoogde aard en werking van hun AI-systemen. Het **post-market** monitoringplan is daarom complementair aan de conformiteitsbeoordeling omdat het gedeeltelijk gebaseerd is op een evaluatie van het AI-systeem voordat het wordt geïmplementeerd.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's
 2. Monitoren van de interne risicobeheersings- en controlesystemen
 3. Afstemmen met Internal Audit
 4. Afstemmen met de externe accountant
 5. Interne en externe verantwoording
 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Bewustwording en AI-vaardigheden van werknemers

AI-geletterdheid

De EU AI Act vereist van alle organisaties dat ze de juiste inspanningen verrichten om ervoor te zorgen dat werknemers voldoende AI-vaardigheden hebben om systemen te begrijpen en effectief te gebruiken, met het oog op een veilig en efficiënt gebruik van AI-systemen in de bedrijfsvoering.

Dit is echter niet de enige reden om ervoor te zorgen dat de AI-geletterdheid van werknemers vergroot wordt. Voor elke baan, functie of rol is de vraag niet óf AI deze zal veranderen, maar wanneer. Het vooralsnog ontbreken van een AI-strategie is geen legitieme reden om te wachten met het aanbieden van bijscholingsmogelijkheden aan werknemers of het creëren van een veilige leeromgeving waarin deze vaardigheden kunnen opbouwen in het gebruik van AI en het omgaan met de risico's van de technologie. Dat laatste is vooral van belang zodat werknemers op eigen initiatief ervaring kunnen opdoen met het gebruik van (generatieve) AI.

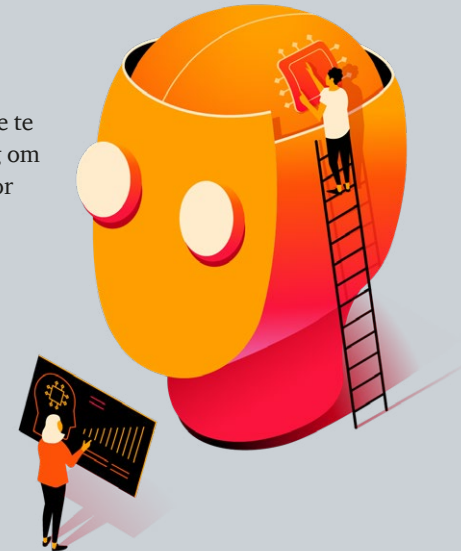
Medewerkers die betrokken zijn bij het uitoefenen van menselijke toezichtactiviteiten met betrekking tot een AI-systeem, zoals de beoordeling van AI-besluitvorming en -uitkomsten, moeten voldoende AI-kennis en training hebben met betrekking tot het AI-

systeem om dergelijke controles effectief uit te voeren. Wendbaarheid is het sleutelwoord hier. Het toepassen van de nieuwste generatie AI-technologie is als het leren samenwerken met een nieuwe ('bekabelde') collega: je moet tijd met elkaar doorbrengen om op elkaar afgestemd te raken. Bij voorkeur is dit al gebeurd voordat de samenwerking dagelijkse realiteit wordt.

Daarnaast kan het nodig zijn om te investeren in nieuwe vaardigheden, gericht op het beheer van technologische AI-risico's.

De rol van de auditcommissie

De auditcommissie kan de raad van bestuur uitdagen op het vraagstuk of de organisatie de juiste expertise en vaardigheden in huis heeft om AI op een verantwoorde manier toe te kunnen toepassen. Het is daarbij van belang om stil te staan bij de vraag wat dit betekent voor de toekomstige samenstelling van teams en talentmanagement.



Waar moet de AI-bijtscholing zich in ieder geval op richten:

- inleiding tot (generatieve) AI en de principes ervan: dit onderwerp geeft een overzicht van (generatieve) AI en legt de fundamentele principes en toepassingen ervan uit. Werknemers leren het potentieel, de voordelen en de uitdagingen begrijpen die gepaard gaan met het gebruik van (generatieve) AI;
- verantwoord gebruik van (generatieve) AI: dit onderwerp benadrukt het belang van verantwoord gebruik van AI. Werknemers leren daarbij onder meer over:
 - juridische kaders waaraan AI-systemen en AI-gebruik dienen te voldoen;
 - ethische overwegingen - waaronder bias, rechtvaardigheid, privacy en transparantie - in de context van AI-gebruik;
 - technisch-inhoudelijke vereisten voor robuuste en veilige AI-systemen.
- **prompt engineering**: gebruikers van generatieve AI-toepassingen leren effectieve prompts of instructies te ontwerpen om het gedrag en de output van AI-modellen te sturen. Werknemers leren hoe ze prompts kunnen schrijven die betrouwbare en ethische AI-resultaten opleveren.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's
 2. Monitoren van de interne risicobeheersings- en controlesystemen
 3. Afstemmen met Internal Audit
 4. Afstemmen met de externe accountant
 5. Interne en externe verantwoording
 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

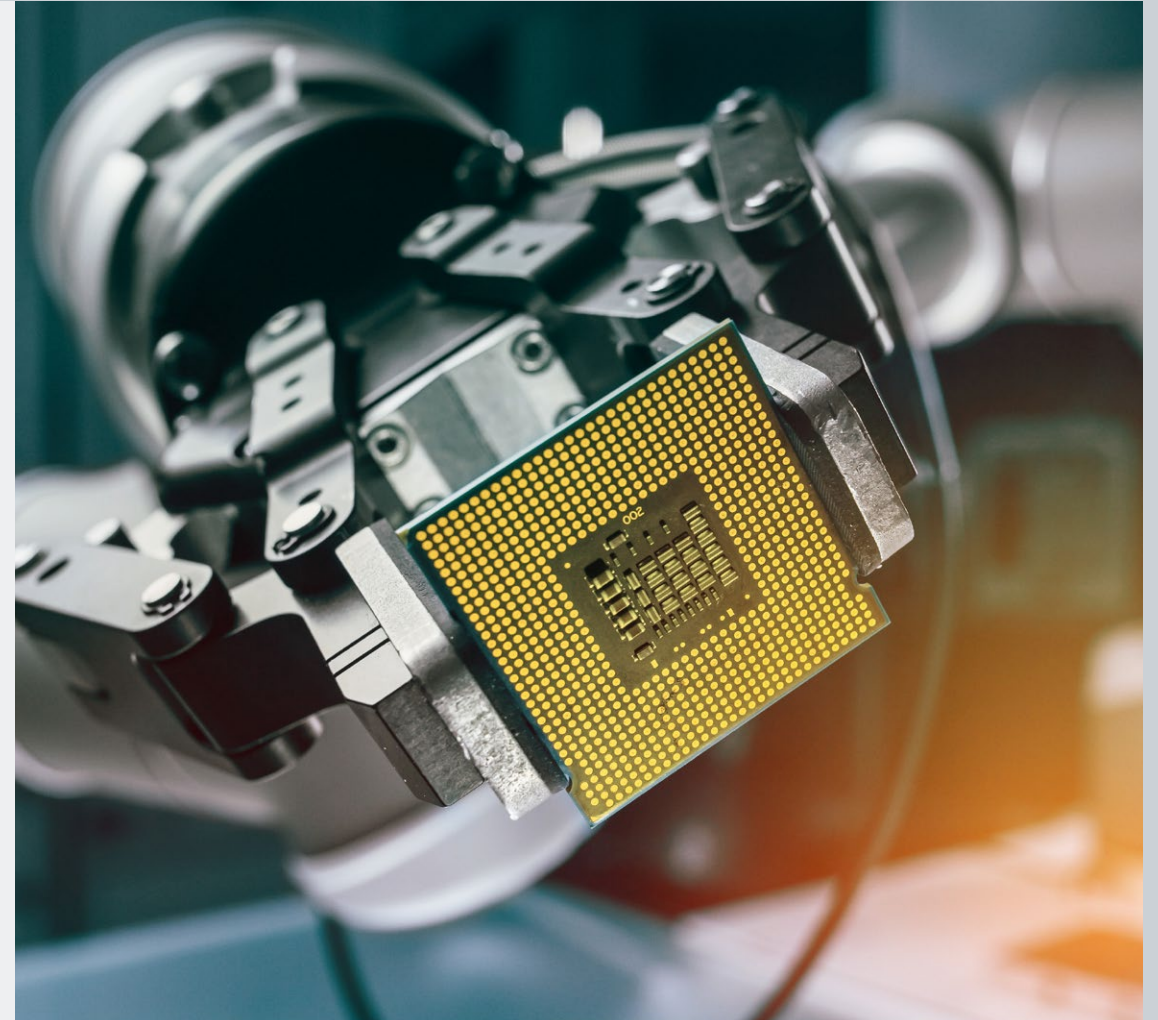
7. Corporate Reporting

8. Crisis

9. Communicatie

Responsible AI: dialoogvragen voor commissarissen en bestuurders

1. Welke kansen/**use cases** zien we voor de toepassing van (Generatieve) AI? Welke innovaties streven we na?
2. Welke rol willen we in onze markt spelen als het op adoptie van (Generatieve) AI aankomt (innovator, early adopter, early majority, late majority, laggard) en waarom?
3. Wat hoopt de organisatie te bereiken met het toepassen van AI, kijkend naar de strategie en de positie op de markt?
4. Welke impact voorzien we op het huidige businessmodel en de manier waarop we met onze klanten en relaties omgaan wanneer de organisatie AI gaat toepassen?
5. Hoe kunnen we data **for good** inzetten? Welke kansen zijn er om als organisatie maatschappelijke impact te maken, bijvoorbeeld in relatie tot ESG-doelstellingen?
6. Op welke plekken binnen de organisatie gaat het toepassen van AI de manier van werken veranderen en hoe nemen we onze mensen hierin mee (inclusief opleiding)?
7. Worden de AI-toepassingen zelf ontwikkeld (al dan niet met inzet van derde partijen) of extern ingekocht? Hoe zijn de voor- en nadelen van het gekozen pad tegen elkaar afgewogen?
8. Zijn we bekend met de minimale vereisten die relevante regelgeving (zoals de AVG, EU Artificial Intelligence Act, Data Act, Data Governance Act) met zich meebrengt? Welke impact van deze regelgeving op de organisatie voorzien we (minimale naleving, bescherming van merk, benutten van nieuwe businesskansen)?
9. Hebben we effectieve processen om te waarborgen dat onze AI-toepassingen (inclusief die van onze leveranciers en samenwerkingspartners in brede zin) opereren in overeenstemming met relevante wet- en regelgeving en **good practices**?
10. Hebben we de juiste expertise en vaardigheden in huis om AI op een verantwoorde manier te kunnen toepassen? Wat betekent dit voor de toekomstige samenstelling van teams en talentmanagement?
11. Hoeveel zijn we bereid te investeren en hoe verdelen we dit over efficiency van processen, klantbeleving, kwaliteit van producten en diensten en nieuwe of verbeterde businessmodellen?
12. Hoe zal de maatschappij kijken naar de wijze waarop wij AI willen inzetten?



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

EU DATA Act

In de snel veranderende wereld van data speelt de auditcommissie een cruciale rol bij het waarborgen van een verantwoorde toepassing van data door organisaties. Met de recente invoering van de EU Data Act wordt deze verantwoordelijkheid nog belangrijker. Auditcommissies moeten zich bewust zijn van de implicaties van de Data Act en hun rol in het toezicht op de naleving ervan. Datamanagement zal de komende jaren een essentiële technologie en drijvende kracht zijn achter digitale transformatie in zowel de publieke als private sector. De verwachting is dat data tegen 2030 een integraal onderdeel zal zijn van alle processen en producten in de Europese waardeketen.

Naast het realiseren van de maatschappelijke en economische voordelen van data, is het essentieel dat stakeholders als klanten en besluitvormers vertrouwen hebben in de rechtmatigheid, eerlijkheid, betrouwbaarheid en beveiliging van datasystemen voor een succesvolle adoptie.

Europese Data Act in het kort
Waar data nu vooral toegankelijk is voor de fabrikanten van apparaten die data genereren, is het doel van de Data Act om bedrijven, burgers en overheden (die de data voornamelijk genereren) meer mogelijkheden te geven om gebruik te maken van data en deze te delen.

Doelen van de Data Act zijn onder andere:

**Data delen:** de bruikbaarheid van data vergroten, obstakels wegnemen en zo extra potentieel ontsluiten door mogelijkheden te creëren voor het hergebruik van data.

**Gebruikersgerichte benadering:** eindgebruikers van digitale producten en diensten centraal plaatsen door hen toegang te geven tot deze data en – onder bepaalde omstandigheden – deze door te geven aan derden.

**Toegankelijkheid door ontwerp:** het zodanig ontwerpen en produceren van Verbonden Producten (zoals hierna gedefinieerd) dat de tijdens het gebruik gegenereerde gegevens standaard gemakkelijk, veilig en - indien nodig - direct toegankelijk zijn voorgebruikers.

**Handelsgeheimen:** adequate bescherming bieden voor handelsgeheimen en intellectuele eigendomsrechten tegen mogelijk misbruik (hoewel de wet gegevensdeling bevordert).

Verbonden Producten
Waar de GDPR zich richt op persoonsgegevens, is de Data Act van toepassing op data die worden gegenereerd door verbonden producten. Dit zijn apparaten die gegevens kunnen genereren, verkrijgen of verzamelen over hun gebruik, prestaties of omgeving en die deze gegevens kunnen communiceren via een kabelgebonden of draadloze verbinding (bijvoorbeeld: slimme huishoudelijke apparaten, consumentenelektronica, industriële machines, medische apparaten, smartphones en tv's).

Op wie van toepassing?
De Data Act is vanaf september 2025 van toepassing op bedrijven die verbonden producten of gerelateerde diensten vervaardigen, partijen die deze gebruiken, overheidsinstellingen en dienstverleners op het gebied van gegevensverwerking.

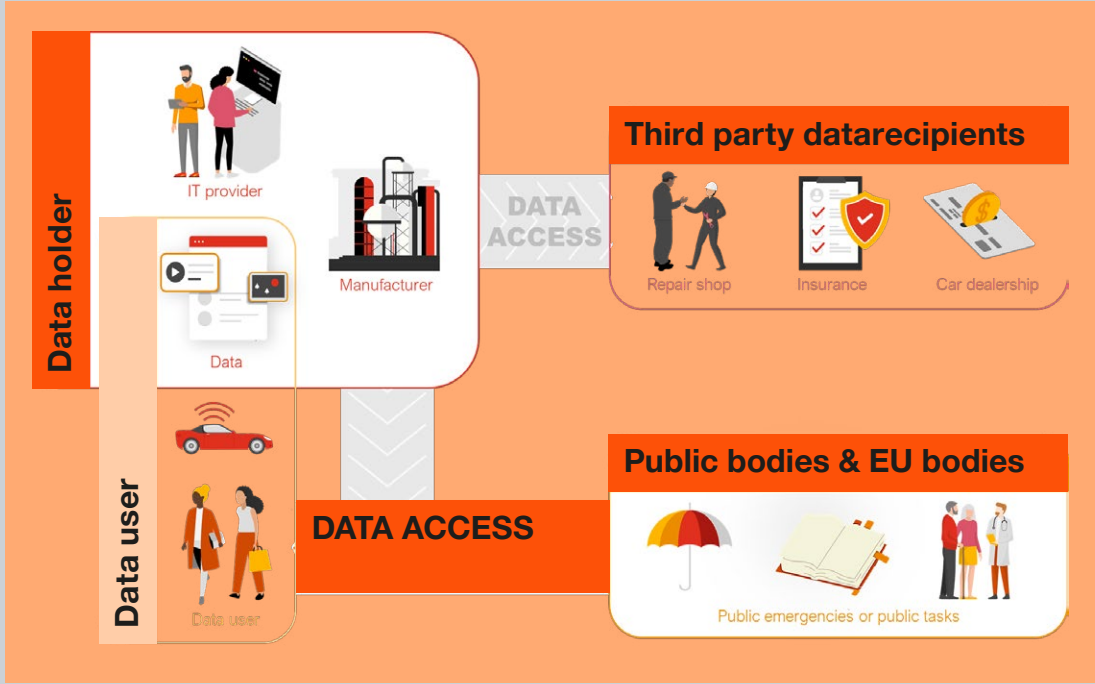
Niet-naleving
Overtredingen die betrekking hebben op persoonsgegevens kunnen leiden tot boetes tot €20 miljoen of 4% van de totale wereldwijde jaaromzet. EU-lidstaten bepalen de sancties voor andere overtredingen. In Nederland kunnen de boetes oplopen tot €1,03 miljoen of 10% van de totale jaaromzet.

Overlap met andere wetten
Cyber Resilience Act - AI Act - Machinery Regulation (EU) 2023/1230 - NIS 2 Directive (EU) 2022/2555 - General Data Protection Regulation (GDPR).

Praktijkvoorbeelden

- Gebruikers kunnen inzicht krijgen in de gegevens van hun apparaten en die gegevens delen met andere partijen (voor bijvoorbeeld reparaties).
- Overheidsinstanties kunnen toegang krijgen tot gegevens als die nodig zijn om te reageren op een openbare noodsituatie (bijvoorbeeld een natuurramp of cyberaanval).
- Overstappen naar een andere cloudprovider moet gemakkelijker worden en verschillende clouddiensten moeten naast elkaar kunnen worden gebruikt.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie



Voor de auditcommissie zijn met name de begrippen relevant die inzicht geven in verantwoordelijkheden en rechten en plichten rond het beheren, delen en gebruiken van data. De volgende definities uit de EU Data Act verdienen extra aandacht:

1. **Datahouder (Data Holder):** De datahouder is degene die daadwerkelijk controle heeft over bepaalde data. Voor de auditcommissie is dit begrip cruciaal, omdat het duidelijk maakt bij wie de verantwoordelijkheid voor databeheer, -toegang, en -bescherming ligt. Het auditen van de borging van integriteit, vertrouwelijkheid en naleving van contractuele en wettelijke verplichtingen begint bij deze rol.
2. **Data-gebruiker (Data User):** De data-gebruiker is de partij met rechtmatige toegang tot data om deze te gebruiken voor specifieke doeleinden. De auditcommissie wil weten hoe de organisatie waarborgt dat data alleen door geautoriseerde gebruikers worden ingezet en of er controlemechanismen zijn om misbruik of overtredingen te signaleren.
3. **Data-ontvanger (Data Recipient):** De data-ontvanger is de partij aan wie de data worden verstrekt, maar die niet de oorspronkelijke eigenaar of houder is. Het is belangrijk om vast te stellen of contractuele afspraken, monitoring en naleving van de vereisten correct zijn vormgegeven. De auditcommissie zal toetsen of de processen rond data-uitwisseling met derden zorgvuldig zijn ingericht en gedocumenteerd.
4. **Data:** Het begrip 'data' zelf is fundamenteel en omvat alle digitale representaties van informatie die door producten of diensten wordt gegenereerd, verzameld of verwerkt. De auditcommissie wil inzicht in de aard, kwaliteit, herkomst en structuur van deze data, omdat dit de basis is van compliance, risico-identificatie en waardebeoordeling.
5. **Data beschikbaar stellen (making data available):** Dit begrip gaat over het proces van het verlenen van toegang tot data aan derden. De auditcommissie verlangt duidelijkheid over de technische en procedurele controls rond data-toegang, omdat hier nalevings- en beveiligingsrisico's spelen die moeten worden gemonitord.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

1. Visie en governance EU Data Act 1/2

Noodzaak van visie en strategie

Voor de auditcommissie is het cruciaal om te waarborgen dat de organisatie over een heldere datastrategie beschikt, die zowel de naleving van de EU Data Act en aanverwante wetten) als de toekomstige groei en wendbaarheid ondersteunt. Het gaat hierbij niet alleen om het formaliseren van beleid en procedures, maar vooral om het stimuleren van een strategische visie op de rol van data binnen alle lagen van de onderneming. Door deze visie vroegtijdig te ontwikkelen en te verankeren in de bedrijfsvoering, kan de organisatie de impact van nieuwe regelgeving voorzien en er proactief op inspelen.

Als toezichthouder op de interne controle- en beheersingsprocessen? heeft de auditcommissie de taak te toetsen of bestuur en management voldoende aandacht besteden aan de waarde van data, het gebruik ervan in besluitvorming en de integratie ervan in kernprocessen. Wanneer deze strategie eenmaal staat, kan de organisatie niet alleen voldoen aan de minimale vereisten van de EU Data Act, maar ook profiteren van efficiencyverbeteringen, beter inspelen op klantbehoeften en kansen creëren voor nieuwe dienstverlening of marktsegmenten. Door de datastrategie te verbinden met de ambities voor de lange termijn, bevordert de auditcommissie dat data-inzet niet beperkt blijft tot incidentele initiatieven, maar structureel

wordt toegepast en geëvalueerd. Zo wordt de organisatie zowel voorbereid op huidige als toekomstige uitdagingen, terwijl deze tegelijkertijd competitief en compliant blijft.

Good practices voor de datastrategie in het licht van de EU Data Act

Doelen en positionering: Formuleer heldere doelstellingen voor datagebruik die aansluiten bij de langetermijnstrategie van de organisatie én de vereisten van de EU Data Act. Denk hierbij aan het versterken van de marktpositie, het creëren van nieuwe diensten op basis van data, of het verbeteren van bestaande producten.

Impact op bedrijfsmodel en klantrelaties: Onderzoek hoe datagebruik – en de verplichtingen tot datadeling – het huidige bedrijfsmodel en de klantinteracties beïnvloeden. Betrek hierbij de eisen rond transparantie, interoperabiliteit en eerlijke contractvoorwaarden: bepaal welke aanpassingen noodzakelijk zijn om compliant te blijven en tegelijk klantwaarde te vergroten.

Maatschappelijke verantwoordelijkheid: Identificeer kansen om data in te zetten voor maatschappelijke impact, bijvoorbeeld in lijn met de Sustainable Development Goals (SDG's) of andere ESG-doelstellingen. Houd rekening met de verwachtingen van de samenleving

rondom ethisch datagebruik en privacy en zorg dat de data-aanpak aansluit op een verantwoord en duurzaam imago.

Organisatorische verandering en mensen meenemen: Bepaal welke afdelingen en functies het meest profiteren van datagedreven werken en zorg voor passende scholing, begeleiding en cultuurverandering. Maak duidelijk welke kennis en vaardigheden nodig zijn om niet alleen aan de EU Data Act (en aanverwante regelgeving) te voldoen, maar ook om data optimaal te benutten in besluitvormingsprocessen.

Investerings en prioritering: Definieer hoeveel middelen worden vrijgemaakt voor data-initiatieven en hoe deze worden verdeeld over efficiencyverbeteringen, klantervaring, productkwaliteit en de ontwikkeling van nieuwe datagedreven businessmodellen. Houd daarbij nadrukkelijk rekening met noodzakelijke investeringen in compliancemaatregelen en IT-infrastructuur die vereisten uit de EU Data Act ondersteunen.

Reputatie en stakeholderperspectief: Overweeg hoe de maatschappij, toezichthouders, investeerders en andere belanghebbenden aankijken tegen het datagebruik. Transparantie, naleving van de EU Data Act en een heldere uitleg van hoe de organisatie data inzet, dragen bij aan vertrouwen en reputatie.

Naleving en datadeling: Stel vast hoe de organisatie aan de verplichtingen uit de EU Data Act zal voldoen, met name rond het rechtmatig delen van data met derde partijen. Zorg voor duidelijke processen, contractuele kaders en controlemechanismen om te garanderen dat data-uitwisseling compliant is en risico's beheersbaar blijven.

Interoperabiliteit en technische randvoorwaarden: Identificeer welke technische standaarden, formats en tools noodzakelijk zijn om te voldoen aan de interoperabiliteitseisen van de EU Data Act. Dit omvat niet alleen aanpasbare IT-architecturen, maar ook robuuste beveiligings- en toegangscontrolesystemen die de integriteit en vertrouwelijkheid van data waarborgen.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Visie en governance EU Data Act 2/2

Effectief toezicht begint op het niveau van de raad van bestuur

De raad van bestuur is uiteindelijk verantwoordelijk voor het gebruik van technologieën en gegevensverwerking binnen de organisatie. Dit vereist dat de raad van bestuur kennis heeft van de EU Data Act om de risico's van het verwerken van gegevens te begrijpen [of te leren zien] en te mitigeren.

De rol van de EU Data Act in effectief toezicht

De EU Data Act speelt een cruciale rol bij het waarborgen van effectief toezicht op het gebruik van gegevens binnen organisaties. Het doel van de EU Data Act is om de bescherming van persoonsgegevens te waarborgen en de rechten van individuen te waarborgen bij het verwerken van hun gegevens. Dit heeft directe implicaties voor het gebruik van technologieën, inclusief AI, aangezien deze vaak afhankelijk zijn van grote hoeveelheden gegevens.

Verantwoordelijkheid door de gehele organisatie

Het afstemmen van de rollen en verantwoordelijkheden van bestaande teams kan een eerste stap zijn om toezicht op gegevensverwerking te ondersteunen. Het is belangrijk dat alle medewerkers zich bewust zijn van hun verantwoordelijkheden met betrekking tot gegevensbescherming en dat er een cultuur

van naleving wordt bevorderd.

Belangrijke aspecten van gegevensgovernance onder de EU Data Act

Onder de EU Data Act moeten organisaties zich houden aan richtlijnen voor gegevensbescherming, naleving van wettelijke vereisten en afstemming op strategische doelstellingen. Het is essentieel dat organisaties een duidelijk kader hebben voor het beheren van gegevensrisico's en ervoor zorgen dat de verantwoordelijkheden en processen worden gedocumenteerd en nageleefd.

Samenwerking tussen verschillende belanghebbenden

Om effectief toezicht op gegevensverwerking te waarborgen, is samenwerking tussen verschillende belanghebbenden van essentieel belang. Dit omvat niet alleen de raad van bestuur en interne teams, maar ook externe partijen als toezichthouders en auditors. Het delen van kennis en ervaring kan helpen bij het identificeren en beheren van gegevensrisico's op een uitgebreide en geïnformeerde manier.

Continue evaluatie en verbetering

Gegevensgovernance is een continu proces dat regelmatige evaluatie en verbetering vereist. Organisaties moeten regelmatig hun gegevensverwerkingsactiviteiten en processen beoordelen om ervoor te zorgen dat ze voldoen aan de vereisten van de EU Data Act

en om eventuele risico's of tekortkomingen aan te pakken. Dit omvat het bijwerken van richtlijnen, het trainen van medewerkers en het implementeren van nieuwe technologieën of methodologieën om de effectiviteit van gegevensgovernance te verbeteren.

De rol van de auditcommissie

De auditcommissie kan de raad van bestuur bijstaan in het vormgeven van een effectieve en robuuste EU Data Act-governancestructuur.

Vragen over de governance rondom de EU Data Act

Om de effectiviteit van de governance en naleving met betrekking tot de EU Data Act binnen een organisatie te beoordelen, kunnen de volgende vragen worden gesteld:

- Welke governancestructuur is ingericht voor de naleving van de EU Data Act? Het is van belang om te begrijpen hoe de organisatie de compliance met de EU Data Act borgt. Dit omvat het identificeren van verantwoordelijke teams, rollen, processen en beleidskaders die betrekking hebben op datagebruik, -deling en -bescherming.
- Is de gehanteerde governancestructuur organisatiebreed toepasbaar op alle data-inzet, of beperkt tot bepaalde soorten data of specifieke gebruiksscenario's? Indien er sprake is van een gefragmenteerde aanpak, is het relevant te onderzoeken hoe de organisatie omgaat met verschillende typen data (bijvoorbeeld interne data, externe data, persoonsgegevens) en of hier uniforme beleidslijnen of aangepaste richtlijnen voor bestaan.
- Wat is het niveau van toezicht en eigenaarschap van de raad van bestuur ten aanzien van de EU Data Act? De mate van betrokkenheid van de raad van bestuur geeft inzicht in de prioriteit die datagovernance en compliance krijgen binnen de organisatie. Een actieve rol van de top kan wijzen op een stevig verankerde strategie en beter toezicht.
- Zijn bestaande governance- en controleraamwerken geactualiseerd om nieuwe verplichtingen uit de EU Data Act te adresseren? Deze kan aanvullende of veranderende risico's en vereisten met zich meebrengen. Het is essentieel dat bestaande raamwerken worden herzien om ervoor te zorgen dat deze voldoen aan de actuele en toekomstige wettelijke eisen.
- Hoe houdt de organisatie toezicht op en en worden risico's beheerd rondom datadeling en -gebruik in bestaande processen en producten, bijvoorbeeld bij het delen van data met ketenpartners, klanten of interne businessunits? Het is belangrijk te bepalen of er heldere processen, controles en escalatiemechanismen zijn om te waarborgen dat bij iedere vorm van datagebruik of -overdracht wordt voldaan aan de vereisten van de EU Data Act.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

- 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Inventarisatie en classificatie van datasystemen

Een grondige inventarisatie van de processen rond datadeling is een essentiële eerste stap om te voldoen aan de EU Data Act. Pas wanneer de organisatie een helder beeld heeft van de soorten beheerde data, de herkomst en bestemming daarvan en de voorwaarden waaronder data wordt gedeeld, kunnen gerichte maatregelen worden getroffen om aan de wettelijke eisen te voldoen. Voor de auditcommissie biedt deze inventarisatie een waardevolle basis om te beoordelen of de interne controles en governance-structuren adequaat zijn ingericht en of er op een consistente manier wordt toegewerkt naar duurzame compliance met de EU Data Act.

Reikwijdte en aanpak

De inventarisatie dient zich niet te beperken tot een enkele databron of één specifiek systeem. Het gaat om een breed onderzoek naar alle interne en externe datastromen, de onderliggende technologie, de betrokken verantwoordelijkheden en de voorwaarden die zijn vastgelegd in contracten en interne beleidslijnen. Hierbij moet inzichtelijk worden welke data de organisatie genereert en gebruikt, welke informatie van buitenaf wordt betrokken en op welke wijze data met externe partijen wordt gedeeld. Het classificeren van data vormt een belangrijk onderdeel van deze exercitie. Door gegevens te ordenen naar type, gevoeligheid, kwaliteit



Welke vragen kan de auditcommissie stellen over datadeling?

Identificeer producten en diensten, analyseer de gegevensstromen en datadeling en stel daarbij de volgende vragen:

- Waar worden data gebruikt binnen de organisatie en welke toepassingen hebben de grootste impact op risico's binnen de organisatie? Wordt data daarbij gedeeld met derden? **Deze vraag helpt de auditcommissie te begrijpen welke datasystemen en toepassingen het meest kritisch zijn voor de organisatie en welke potentiële risico's ze met zich meebrengen.**
- Blijft de organisatie bijhouden welke datatechnologie er wordt gebruikt? **Het is belangrijk voor de auditcommissie om te weten hoe de organisatie het gebruik van datatechnologieën monitort en bijhoudt, om ervoor te zorgen dat alle systemen compliant blijven met de EU Data Act.**
- Worden de datatoepassingen zelf ontwikkeld (al dan niet met inzet van derde partijen) of extern ingekocht? **Het is belangrijk om te weten of datasystemen intern worden ontwikkeld of extern worden ingekocht, omdat dit invloed kan hebben op de nalevingsvereisten en de risico's die aan deze systemen verbonden zijn.**

en eigendomsrechten wordt duidelijk waar de grootste risico's en kansen liggen. Het opstellen van procesoverzichten en dataschema's helpt om de complexiteit van interne datastromen te ontrafelen, zodat de organisatie inzicht krijgt in waar data vandaan komen, hoe deze worden verwerkt en waar deze uiteindelijk naartoe gaan. Deze inspanning is niet eenmalig: regelmatige herziening en bijstelling zijn nodig om in te spelen op organisatorische veranderingen, nieuwe samenwerkingsverbanden, technologische ontwikkelingen en wijzigingen in de regelgeving.

Identificatie van risico's en compliance-eisen

Zodra de datastromen in kaart zijn gebracht, ontstaat een fundament om risico's en compliancevraagstukken beter te begrijpen. De EU Data Act vereist onder meer dat data kwalitatief goed, betrouwbaar en toegankelijk zijn. Ook vraagt de wet om een transparante, eerlijke en veilige manier van datadeling met derden. Door de inventarisatie te koppelen aan de bepalingen van de EU Data Act, kan de organisatie knelpunten signaleren, zoals ongeautoriseerde toegang tot data, gebrekkige kwaliteitscontroles of onvoldoende heldere contractuele afspraken met externe partijen. Het inventariseren van deze risico's biedt niet alleen inzicht in waar de organisatie verbeteringen moet doorvoeren, maar ook in welke mate de bestaande interne controlemechanismen, zoals beleid, procedures en interne audits, aansluiten

1. **Commissie**
2. **Continuïteit**
3. **Corporate impact**
4. **Control & Compliance**
 1. Beoordelen van de risico's
 2. Monitoren van de interne risicobeheersings- en controlesystemen
 3. Afstemmen met Internal Audit
 4. Afstemmen met de externe accountant
 5. Interne en externe verantwoording
6. **Enkele risicocategorieën uitgelicht**
Bijlagen
5. **Cultuur en gedrag**
6. **Checks & Balances**
7. **Corporate Reporting**
8. **Crisis**
9. **Communicatie**

op de nieuwe wettelijke verplichtingen. Zo kan de organisatie gericht werken aan het dichten van eventuele lacunes, het aanscherpen van bestaande maatregelen en het versterken van de algehele governance rond data. Hierbij is het van cruciaal belang om de overlap met andere wet- en regelgeving (zoals de AVG) in kaart te brengen.

Documentatie, rapportage en toegevoegde waarde

De resultaten van de inventarisatie moeten op een inzichtelijke manier worden gedocumenteerd en periodiek worden gerapporteerd aan de relevante belanghebbenden, waaronder de auditcommissie. Heldere rapportages, ondersteund door kernindicatoren en doorlopende monitoring, stellen de auditcommissie in staat om te beoordelen of de organisatie effectief toewerkt naar structurele naleving van de EU Data Act. Bovendien dient deze vastlegging niet alleen als verantwoording naar interne toezichthouders en bestuur, maar ook als basis voor toekomstige externe audits en eventuele vragen van toezichthouders. Het voordeel van een grondige inventarisatie strekt verder dan puur legalistische naleving. Door inzichtelijk te maken welke data de organisatie beheert en in welke processen deze worden ingezet, kan inefficiëntie worden opgespoord, kunnen kansen worden geïdentificeerd om de dataverwerking te optimaliseren en kan het fundament voor een bredere datastrategie worden gelegd. De auditcommissie kan in haar rol als toezichthouder

en adviseur het bestuur hierop wijzen, zodat inzichten uit de inventarisatie niet alleen leiden tot compliance, maar ook tot een sterkere, datagedreven organisatie.

■ **De rol van de auditcommissie**
Het is van belang dat de auditcommissie betrokken is bij het beoordelen van de risico's die datasystemen met zich meebrengen,

vanuit haar rol in de voorbereiding van de besluitvorming door de raad van commissarissen over niet-financiële thema's, zoals datagovernance.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's
 2. Monitoren van de interne risicobeheersings- en controlesystemen
 3. Afstemmen met Internal Audit
 4. Afstemmen met de externe accountant
 5. Interne en externe verantwoording
 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Compliance EU Data Act

De EU Data Act stelt nieuwe eisen aan de manier waarop organisaties data verzamelen, delen en beschermen, met als doel een rechtvaardig en transparant datadeling-ecosysteem. Voor de auditcommissie is het essentieel te begrijpen welke verplichtingen de EU Data Act met zich meebrengt en te toetsen of de interne controles, governance en rapportagestructuren aansluiten op deze vereisten. Deze paragraaf biedt een raamwerk om de organisatie voor te bereiden op naleving, met nadruk op de rol van de auditcommissie.

Begrip van reikwijdte en vereisten

De EU Data Act verlangt dat data toegankelijk en overdraagbaar zijn en dat contractuele afspraken over datadeling eerlijk en transparant worden opgesteld. Tegelijkertijd moet de organisatie vertrouwelijkheid en intellectuele eigendomsrechten respecteren. De auditcommissie toetst of het management deze verplichtingen correct interpreteert, kennis intern verspreidt en waar nodig beleid en processen aanpast.

Governance en verantwoordelijkheidstoedeling

Een heldere toedeling van verantwoordelijkheden is onmisbaar. Het benoemen van een data compliance officer, het structureren

van samenwerking tussen juridische, IT-, compliance- en privacyteams en het vastleggen van rapportagelijnen zorgen voor een solide basis. De auditcommissie kan door middel van kritische vragen en interne audits verifiëren of de governancestructuur daadwerkelijk functioneert.

Van theorie naar implementatie

Naast beleidsvorming is praktische uitvoering cruciaal: het inventariseren van datastromen, het beoordelen van contracten met derde partijen en het zorgen dat technische systemen voldoen aan interoperabiliteitseisen. Trainingen voor medewerkers en bewustwordingsprogramma's helpen de naleving duurzaam te verankeren. De auditcommissie ziet erop toe dat deze initiatieven leiden tot effectieve en toekomstbestendige naleving.

Inventarisatie en classificatie van data

De organisatie moet exact weten over welke data wordt beschikt, waar deze vandaan komen welke rechten eraan verbonden zijn en aan welke wettelijke verplichtingen men moet voldoen. Dit begint met een grondige **data mapping**, gevolgd door een zorgvuldig classificatieproces om de vertrouwelijkheid en juridische kaders te bepalen. Ook het opstellen en naleven van een dataretentiebeleid is hierbij van belang. De auditcommissie ziet erop toe dat deze inventarisatie actueel en volledig is en dat de classificatiecriteria helder en consequent worden toegepast.

Welke vragen kan de auditcommissie stellen over de naleving van de EU Data Act?

- Hoe worden de datastromen en de dataverwerking binnen de organisatie continu gemonitord om naleving van de EU Data Act te waarborgen?
- Zijn bestaande controlemechanismen, interne audits en rapportagetools voldoende om tijdig signalen van non-compliance op te vangen?
- Welke maatregelen zijn geïmplementeerd om datakwaliteit en integriteit te behouden en hoe wordt getest of deze maatregelen in de praktijk effectief zijn?
- Is er een duidelijk escalatie- en sanctioneringsmechanisme voor het geval dat nalevingsproblemen worden geïdentificeerd en zijn de verantwoordelijken op de hoogte van hun rol hierin.
- In hoeverre wordt periodieke (bij)scholing ingezet om medewerkers up-to-date te houden over wijzigingen in de EU Data Act, nieuwe best practices en ontwikkelingen in technische standaarden?
- Hoe borgt de organisatie dat alle contractuele afspraken met externe partijen in lijn blijven met de wettelijke eisen, ook als deze externe partijen of marktomstandigheden veranderen?



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's
 2. Monitoren van de interne risicobeheersings- en controlesystemen
 3. Afstemmen met Internal Audit
 4. Afstemmen met de externe accountant
 5. Interne en externe verantwoording
 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Technische en organisatorische maatregelen

Om aan de EU Data Act te voldoen, zijn zowel technische als organisatorische voorzieningen nodig. Denk aan interoperabiliteitsstandaarden die aansluiten bij Europese richtlijnen, gedegen beveiligingsmaatregelen (waaronder toegangscontrole en encryptie) en een robuust continuïteitsplan voor data-uitwisseling bij incidenten. De auditcommissie beoordeelt of deze maatregelen daadwerkelijk op een effectieve en duurzame manier zijn geïmplementeerd.

■ De rol van de auditcommissie

Voor een succesvolle naleving van de EU Data Act is het van cruciaal belang dat de auditcommissie nauw betrokken is bij zowel de voorbereiding als de daadwerkelijke borging van compliance. Dit betekent dat zij een actieve rol moet spelen in de beoordeling en aanscherping van de bestaande controlesystemen. Daarnaast houdt de auditcommissie toezicht op de ontwikkeling en implementatie van nieuwe processen, beleidslijnen en procedures die de organisatie in staat stellen te voldoen aan de vereisten van de EU Data Act. Op deze manier kan de auditcommissie bijdragen aan een solide governancestructuur, transparantie en duurzaam datagebruik binnen de organisatie.

Welke vragen kan de auditcommissie stellen over de voorbereiding op de EU Data Act?

- Op welke manier brengt de organisatie in kaart welke data worden verzameld en gebruikt hoe wordt vastgesteld of deze data binnen de reikwijdte van de EU Data Act vallen?
- In hoeverre zijn bestaande contracten, interne beleidslijnen en procedures al afgestemd op de eisen van de EU Data Act en waar zijn aanpassingen nodig?
- Is er een helder inzicht in de rollen en verantwoordelijkheden rond databeheer, toezicht, rapportage en besluitvorming en zijn deze schriftelijk vastgelegd?
- Welke technische aanpassingen zijn nodig om te voldoen aan de interoperabiliteitsvereisten en om data veilig, consistent en toegankelijk te houden?
- Hoe worden medewerkers opgeleid en geïnformeerd over de inhoud en implicaties van de EU Data Act en zijn er plannen voor continue bijscholing?
- Is er een strategie of **roadmap** opgesteld om actief in te spelen op toekomstige wijzigingen in de EU Data Act of aanvullende regelgeving, zodat de organisatie wendbaar blijft en tijdig kan bijsturen?



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

4. Bewustwording en vaardigheden medewerkers

De EU Data Act stelt organisaties voor de uitdaging om hun omgang met data naar een hoger niveau te tillen. Dit gaat niet alleen over het formaliseren van beleid en procedures, maar vooral over het creëren van een cultuur waarin werknemers begrijpen wat de wettelijke eisen zijn en weten hoe ze data op een zorgvuldige, transparante en efficiënte manier kunnen gebruiken. Voor de auditcommissie is het van belang te toetsen of de organisatie in voldoende mate investeert in kennisopbouw, vaardigheden en bewustwording, zodat medewerkers zelfstandig kunnen opereren binnen de kaders van de EU Data Act.

Datageletterdheid en compliance

De EU Data Act legt nadruk op het verantwoord gebruiken, delen en beschermen van data. De regelgeving schrijft geen expliciete trainingen voor, maar impliceert wel dat organisaties hun personeelsbestand op de hoogte brengen van de relevante verplichtingen:

• Rechten en plichten bij datadeling:

Medewerkers moeten bekend zijn met de voorwaarden waaronder data met derden mogen worden gedeeld en welke waarborgen nodig zijn om intellectuele eigendomsrechten en vertrouwelijkheid te respecteren.

• Datakwaliteit en -integriteit:

Medewerkers dienen te weten hoe zij data controleren, opschonen en beheren,

om zo te voldoen aan de kwaliteits- en interoperabiliteitseisen van de EU Data Act.

• Datagovernance en verantwoordingsplicht:

Medewerkers moeten inzicht hebben in de interne governance-structuren, verantwoordelijkheden en controlemechanismen, zodat zij begrijpen wie waarover rapporteert, hoe incidenten gemeld worden en hoe naleving wordt bewaakt.

Van theorie naar praktijk

Medewerkers kunnen alleen effectief bijdragen aan compliance als zij niet alleen weten wat de regels zijn, maar ook begrijpen waarom deze regels gelden en hoe ze in de dagelijkse praktijk kunnen worden toegepast. Dit betekent dat de organisatie:

• Praktijkgerichte trainingen

aanbiedt om datagerelateerde vaardigheden op te bouwen, zoals het werken met gestandaardiseerde dataformaten, het correct toepassen van toegangsbeperkingen, en het signaleren van datalekken of onrechtmatig gebruik.

• Interne kennisdeling

stimuleert, bijvoorbeeld door interne seminars, FAQ-lijsten en digitale kennisplatformen op te zetten. Zo wordt het eenvoudiger voor medewerkers om ervaringen uit te wisselen en gezamenlijk te leren.

• Scenario-based leren

bevordert, waarin concrete voorbeeldcases worden besproken: hoe ga je om met een dataverzoek van een externe partij, hoe controleer je of de data voldoende kwaliteit hebben, hoe herken je situaties waarin aanvullende

veiligheidsmaatregelen nodig zijn?

De rol van de auditcommissie

De auditcommissie kan de raad van bestuur uitdagen om te beoordelen of de organisatie beschikt over de juiste expertise en vaardigheden om aan de vereisten van de EU Data Act te voldoen. Dit gaat verder dan enkel kennis van wet- en regelgeving; het omvat ook technische competenties rondom datakwaliteit,

interoperabiliteit en veilig datagebruik, evenals juridische en ethische overwegingen. Het is daarbij van belang om stil te staan bij de toekomstige samenstelling van teams en de strategie voor talentmanagement. Indien er hiaten zijn in de kennis of vaardigheden, kan het nodig zijn om gericht te investeren in bijscholing of het aantrekken van gespecialiseerd personeel, zodat de organisatie optimaal voorbereid is op de uitdagingen van de EU Data Act.

Continu leren en bijscholen

De EU Data Act maakt deel uit van een dynamisch regelgevingsveld waarin standaarden, technische vereisten en interpretaties kunnen wijzigen naarmate de markt en technologie zich ontwikkelen. Dit vraagt om een cultuur van doorlopende professionalisering en bijscholing binnen de organisatie, gericht op het up-to-date houden van kennis en vaardigheden.

• periodieke bijscholingsprogramma's:

het organiseren van regelmatige trainingen en e-learning's om medewerkers te informeren over gewijzigde of aangescherpte vereisten uit de EU Data Act, bijvoorbeeld bij herzieningen van datadelingsovereenkomsten, nieuwe interoperabiliteitsstandaarden of aanpassingen in toezichtkaders;

• regelmatige evaluaties van leertrajecten:

continue monitoring en evaluatie van de bestaande opleidingsinspanningen, waarbij wordt gecontroleerd of de inhoud nog aansluit op de actuele eisen van de EU Data Act. Zo kan de organisatie tijdig inspelen op leemtes in kennis of vaardigheden;

• inzet van experts en interne kennisdeling:

laat interne en externe specialisten workshops of masterclasses te verzorgen voor bewustzijn en diepgaande kennis over complexe onderwerpen, zoals nieuwe datakwaliteitsrichtlijnen of contractuele verplichtingen. Stimuleer tevens interne kennisuitwisseling, bijvoorbeeld via vakgroepen of communities of practice, om best practices rondom de naleving van de EU Data Act te delen.

Door deze gerichte, continue bijscholing blijven alle medewerkers in de organisatie niet alleen op de hoogte van de laatste ontwikkelingen, maar zijn ze ook beter in staat om de EU Data Act structureel en proactief in de dagelijkse praktijk te verankeren.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

5. Integriteitsschending en frauderisico's

Interne risicobeheersings- en controlesystemen worden primair ontwikkeld om de organisatie in staat te stellen de strategische doelen te realiseren en de risico's te verkleinen die de realisatie van deze doelen in de weg staan. De interne risicobeheersings- en controlesystemen zijn onder meer gericht op bescherming tegen fouten of fraude. Zelfs met de best ontworpen systemen kan echter niet worden gegarandeerd dat de interne controle- en beheersingsmaatregelen niet zullen worden geschonden, verkeerd begrepen of verkeerd geïnterpreteerd.

De auditcommissie zal dan ook voortdurend alert zijn op integriteits- en frauderisico's, om mogelijke onregelmatigheden vroegtijdig te signaleren en aan te pakken. In deze paragraaf gaan we in op hoe de auditcommissie fraude en integriteitsschendingen kan proberen te voorkomen. Hoofdstuk 8 (Crisis – wat te doen bij misstanden en onregelmatigheden?) behandelt onder meer de vraag hoe de auditcommissie kan handelen wanneer er fraude of een integriteitsschending is geconstateerd.

Monitoring interne risicobeheersings- en controlesystemen

Bij de monitoring van de interne

risicobeheersings- en controlesystemen houdt het bestuur volgens de Code rekening met geconstateerde zwaktes, misstanden en onregelmatigheden, signalen van klokkenluiders, geleerde lessen en bevindingen van Internal Audit en de externe accountant. Waar nodig worden verbeteringen doorgevoerd.

De rol van de auditcommissie

De auditcommissie houdt toezicht op de monitoring van risicobeheersing en interne controle door het bestuur. Het gaat bij (niet-) naleving echter niet alleen om systemen en hard controls, het gaat ook om mensen en soft controls. De auditcommissie kijkt dus verder dan alleen naar de interne risicobeheersings- en controlesystemen en houdt ook de organisatiecultuur en het gedrag regelmatig tegen het licht. Daarbij kunnen de volgende vragen behulpzaam zijn:

- Hoe is de toon aan de top? Is het ethisch normbesef in de bestuurskamer en in de rest van de organisatie goed ontwikkeld?
- Kenmerkt de organisatie zich door een (on)gezonde cultuur en bijbehorend gedrag?
- Leven kernwaarden en de gedragscode daadwerkelijk, of zijn het dode letters?
- Kan er open worden gesproken over fouten?
- Durven mensen gebruik te maken van de klokkenluidersregeling: worden meldingen opgevolgd? Of zijn er juist niet of nauwelijks meldingen? Dat kan een indicatie zijn dat medewerkers zich niet vrij voelen om hun zorgen te delen.

Zie verder hoofdstuk 5: Cultuur en gedrag

Beloningsstructuur als risico

De Code noemt expliciet de beloningsstructuur van bestuurders en werknemers als een te identificeren en beheersen risico. Als deze verkeerde prikkels bevat, kan dat immers leiden tot ongewenst gedrag van bestuurders en medewerkers en het nemen van ongewenste en onverantwoorde risico's en mogelijk zelfs integriteitsschending of fraude. Opvallend genoeg verbreedt de Code het risico van de beloningsstructuur niet tot cultuur- en gedragsrisico's in het algemeen, terwijl wel wordt aangegeven dat een gezonde cultuur misstanden en onregelmatigheden kan helpen voorkomen. Het is dus verstandig om ook te kijken naar cultuur en gedrag bij de risicobeoordeling en alert te zijn op red flags voor fraude en integriteitsschendingen: in de boardroom en daarbuiten.

Frauderisicoanalyse

De auditcommissie zal kennis willen nemen van de door het bestuur opgestelde frauderisicoanalyse. In de bespreking van deze analyse met het bestuur zal de auditcommissie haar eigen kennis en ervaring met de onderneming en de sector gebruiken om vast te stellen of de frauderisicoanalyse een goede weergave is van de meest significante frauderisico's, de daarbij behorende interne controlemaatregelen en de weging van het restrisico in het licht van de **risk appetite** van de onderneming. Aandachtspunten en handvatten

met betrekking tot frauderisicoanalyse kunt u via deze [link](#) raadplegen.

Niet-financiële informatie

Met de CSRD zal er de komende tijd meer en meer aandacht komen voor het rapporteren van niet-financiële informatie (bijvoorbeeld inzake klimaatdoelstellingen). De auditcommissie zal zich ervan moeten vergewissen dat de door het bestuur gepresenteerde niet-financiële informatie een betrouwbaar en realistisch beeld geeft en er geen sprake is van 'greenwashing'. Ook hier dient de auditcommissie haar kennis en ervaring van de onderneming en de sector in te zetten om de betrouwbaarheid van deze informatie te beoordelen.

Risico van het doorbreken van interne beheersingsmaatregelen door het bestuur

De auditcommissie dient ook beducht te zijn op het risico dat het bestuur de maatregelen van interne beheersing doorbreekt. Bijvoorbeeld als het bestuur zichzelf of de onderneming wil bevoordelen of de financiële positie van de onderneming anders wil voorstellen dan dat deze daadwerkelijk is (zie ook risicocategorie 6 over verslaggevingsrisico's). Hoewel het lastig kan zijn dit te signaleren dient de auditcommissie open te staan voor signalen die in deze richting wijzen en daarop te acteren. In het kader van de financiële verantwoording dient de auditcommissie zich een beeld te vormen van de significante schattingsposten en de daaraan ten grondslag liggende veronderstellingen.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Overleg met de externe accountant

Naast de door het bestuur verstrekte en zelf vergaarde informatie, eigen observaties en ondersteuning door Internal Audit kan de auditcommissie gebruikmaken van de observaties van de externe accountant bij de frauderisicoanalyse tijdens de controlewerkzaamheden. De auditcommissie kan ook tijdens een **private session** met de externe accountant vragen naar diens indruk van de cultuur en mogelijke integriteitsrisico's. Vermoedens van fraude worden altijd gemeld door de accountant aan de raad van commissarissen

en de auditcommissie. Boekhoudfraude komt in risicocategorie 6 over verslaggevingsrisico's aan de orde.

De auditcommissie kan de externe accountant tijdens het overleg ook vragen om aandacht te besteden aan om aandacht te besteden aan specifieke onderwerpen die de auditcommissie van belang acht. Hierbij kan bijvoorbeeld gedacht worden aan een **deep dive** in bepaalde processen of het beoordelen van de declaraties van het management.

6. Verslaggevingsrisico's

Transparantie en het afleggen van verantwoording zijn kernbegrippen in goed bestuur. De integriteit en de kwaliteit van de financiële verslaggeving moeten zijn gewaarborgd. Het is de enige risicocategorie waarvoor de Code specifiek de doelstelling van de interne beheersing en controle benoemt: de systemen moeten een redelijke mate van zekerheid geven dat de financiële verslaggeving

geen onjuistheden van materieel belang bevat. Het bestuur stelt dit vast en verklaart vervolgens in het bestuursverslag dat dit het geval is, voorzien van een duidelijke onderbouwing. De auditcommissie houdt toezicht op de integriteit en kwaliteit van de financiële verslaggeving. Daarbij hoort alertheid op risico's die die integriteit en kwaliteit kunnen bedreigen.

Onjuistheden van materieel belang

De externe accountant die de controle uitvoert, is verantwoordelijk voor het verkrijgen van een redelijke mate van zekerheid dat de jaarrekening als geheel geen afwijkingen van materieel belang bevat, als gevolg van fraude of fouten.

Wat mag de auditcommissie verwachten van de externe accountant bij frauderisico's?

Bij de risicoanalyse als onderdeel van het controleplan

- Als onderdeel van elke controle worden de frauderisicofactoren bij de klant in kaart gebracht. Hierin worden de frauderisicofactoren uit de (bijlage van de) controlestandaarden betrokken, evenals de voor de desbetreffende branche en organisatie specifieke frauderisicofactoren. De accountant zal vervolgens evalueren of de informatie die is verkregen uit risico-inschattingswerkzaamheden wijst op het bestaan van een of meer frauderisico's. Daarnaast kijkt de accountant naar de interne beheersingsmaatregelen die de klant heeft ingericht.
- De accountant neemt kennis van de beschouwing van de frauderisico's door de organisatie zelf en gebruikt deze voor/vergelijkt deze met zijn eigen frauderisicoanalyse. Het proces van de frauderisicoanalyse wordt besproken met de auditcommissie en idealiter ook met de voltallige raad van commissarissen.
- De accountant communiceert met het bestuur en/of interne toezichthouders relevante zaken rondom fraude en frauderisico's. Dit geldt ook indien de organisatie zelf de frauderisico's niet of onvoldoende in beeld heeft. Het bestuur en de interne toezichthouders zijn en blijven immers verantwoordelijk voor de opzet, de implementatie en de werking van een stelsel van interne beheersing dat afwijkingen in de financiële overzichten kan voorkomen, detecteren en/of corrigeren.

Bron: Fraudeprotocol NBA (de Koninklijke Nederlandse Beroepsorganisatie van Accountants)

Verslaggevingsrisico's: waar kan de auditcommissie op letten?

- Begrijp de impact van de strategie op de financiële positie en de verslaglegging.
- Focus op frauderisico's in financiële verslaglegging: bevraag het bestuur kritisch op de frauderisicoanalyse.
- Beoordeel en begrijp de meldingen via de klokkenluidersregeling.
- Doorgrond de transacties met verbonden partijen en significante niet-routinematige transacties.
- Bespreek periodiek met het bestuur de controleomgeving en de fraudepreventieprogramma's.
- Beoordeel periodiek de integriteit van het bestuur.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

- 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Het verschil tussen **fraude** en **onjuistheden** in de jaarrekening: is de afwijking in de jaarrekening opzettelijk of onopzettelijk? Fraude is opzettelijke misleiding om onrechtmatig voordeel te verkrijgen.

Belangrijkste risico's in de verslaggeving

- gevaar van discontinuïteit, leidend tot bijvoorbeeld het manipuleren van de cijfers om te voldoen aan vereisten van bankconvenanten en het beïnvloeden van kasstromen;
- willen voldoen aan verwachtingen van analisten;
- persoonlijke drijfveren van bestuurders en het management, waaronder het maximeren van bonussen en beloning;
- achterhouden van slecht nieuws zoals het verslechteren van de financiële positie;
- beïnvloeden van de ontwikkeling van de koers van de aandelen;
- oppoetsen van de financiële positie met het oog op een komende aandelenuitgifte, het aantrekken van een nieuwe lening of een mogelijke acquisitie.

Aanwijzingen voor fraude

De externe accountant zal tijdens de controle het risico inschatten van een afwijking van materieel belang als gevolg van fraude en hiertoe voldoende en geschikte controle-informatie verzamelen. Als er aanwijzingen of vermoedens zijn van fraude bespreekt de externe accountant deze met de bestuurders, ongeacht of de mogelijke fraude wel of niet van materieel belang is voor de jaarrekening.

Ook de voorzitter van de auditcommissie wordt onmiddellijk geïnformeerd. Wanneer (het vermoeden van) een misstand of onregelmatigheid het functioneren van een bestuurder betreft, meldt de externe accountant dit aan de voorzitter van de raad van commissarissen. Zie hoofdstuk 8 voor hoe te handelen in het geval van een crisis, bijvoorbeeld als gevolg van misstanden en onregelmatigheden.

Wat mag de auditcommissie verwachten van de externe accountant bij frauderisico's?

Tijdens de controle

- De accountant voert passende controlewerkzaamheden uit, die zijn gericht op het ondervangen van de frauderisico's die kunnen leiden tot een afwijking van materieel belang in de jaarrekening Voor de accountant is een frauderisico altijd een belangrijk risico (een zogenaamde 'significant risico'). De accountant zorgt elk jaar voor een element van onvoorspelbaarheid in de aard, timing en omvang van de controlewerkzaamheden. De werkzaamheden vormen een onderdeel van het controleplan, dat afgestemd wordt met het relevante orgaan van de klant (bestuurders en/of de auditcommissie).
- De accountant is alert op mogelijke aanwijzingen voor fraude. Zo bespreekt de accountant bijvoorbeeld de meldingen die ontvangen zijn via een klokkenluidersregeling, plus interne onderzoeken die worden uitgevoerd rondom fraude(risico's). Hij of zij kan ook data-analyse inzetten om afwijkingen, die mogelijk het gevolg zijn van fraude, op het spoor te komen. De accountant zorgt bij de uitvoering van die werkzaamheden, ondersteund door de accountantsorganisatie, voor een passende teambezetting, zo nodig met de inzet van forensische expertise.
- De accountant zal altijd controlewerkzaamheden verrichten die gericht zijn op het frauderisico dat het management de interne beheersing doorbreekt. Deze zien ten minste toe op:
 - het toetsen of de in het grootboek vastgelegde journaalposten en andere aanpassingen die tijdens het opstellen van de financiële overzichten zijn aangebracht aanvaardbaar zijn;
 - het beoordelen van schattingen op tendenties en of de eventuele omstandigheden die tot de tendentie hebben geleid een risico vormen op een afwijking van materieel belang die het gevolg is van fraude;
 - het beoordelen van significante transacties die buiten het kader van de normale bedrijfsvoering vallen, of die in een ander opzicht ongebruikelijk lijken in het licht van zowel het inzicht van de accountant in de organisatie en de omgeving, als andere tijdens de controle verkregen informatie: doen de zakelijke beweegredenen (of het ontbreken daarvan) voor deze transacties vermoeden dat ze mogelijk zijn aangegaan met het oog op frauduleuze financiële verslaggeving of het verhullen van een oneigenlijke toe-eigening van activa?
- Elke aanwijzing van fraude wordt besproken met de bestuurders en/of de auditcommissie. Accountants geven aan welke acties ten minste genomen moeten worden. De organisatie is zelf verantwoordelijk voor het onderzoek naar de aard en omvang van de fraude.

Bron: Fraudeprotocol NBA.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
- 6. Enkele risicocategorieën uitgelicht
 - Bijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

7. Corruptierisico's

Bij corruptie gaat het om handelingen die verband houden met het doen van een gift of een belofte om de ander (een ambtenaar of een privaatrechtelijke persoon of partij) te verleiden iets te doen of na te laten. Bij zogenaamde **facilitation payments** gaat het om betalingen van kleinere bedragen aan ambtenaren om handelingen te versnellen. Corruptie houdt vaak ook verband met vraagstukken op het gebied van belangenverstrengeling (vermenging van zakelijke en privébelangen). Er bestaat onderscheid tussen actieve en passieve corruptie. Passief heeft betrekking op het ontvangen van bijvoorbeeld steekpenningen, actief op het betalen daarvan.

De internationalisering van het zakendoen heeft geleid tot een toename van het corruptierisico. Internationale activiteiten vinden plaats op grotere afstand van het hoofdkantoor, waardoor misstanden en onregelmatigheden met betrekking tot corruptie en omkoping zich gemakkelijker aan het zicht kunnen onttrekken. Bovendien worden er in het buitenland soms andere normen en waarden gehanteerd, waarmee organisaties bij het zakendoen worden geconfronteerd.

Ook corruptierisico in de keten

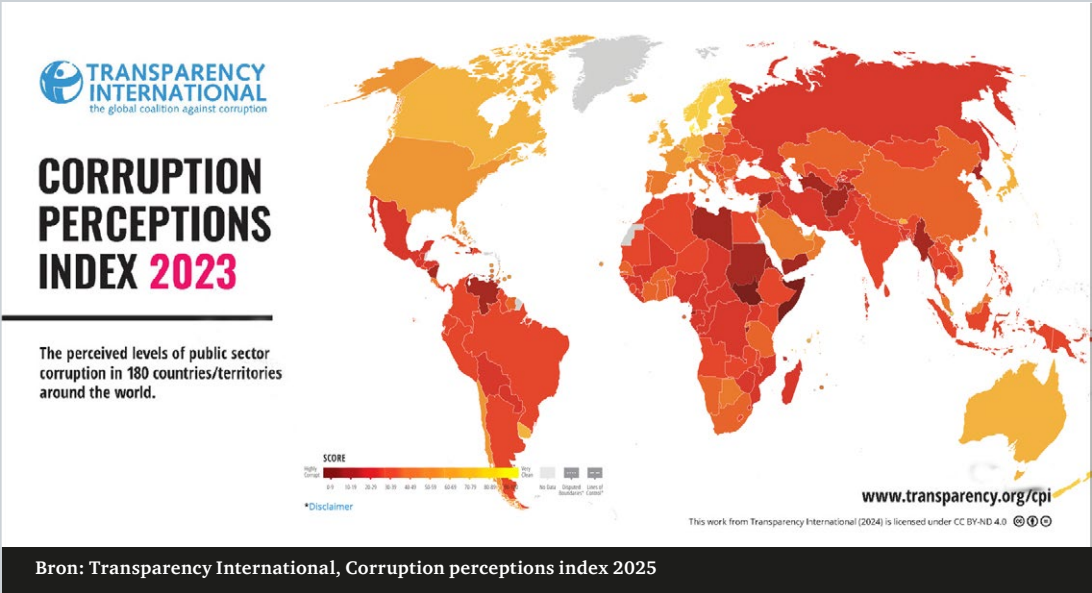
Corruptie is strafbaar volgens Nederlandse en internationale wetgeving. Corruptie brengt dus een compliancerisico met zich mee, wat gepaard kan gaan met reputatieschade en hoge boetes. Daarnaast kunnen organisaties of betrokken medewerkers hun onafhankelijkheid en legitimiteit verliezen door corruptie en doordat ze chantabel worden. Organisaties lopen niet alleen corruptierisico bij hun eigen medewerkers, maar ook in de keten: bij leveranciers, agenten en distributeurs. Bij een effectief anti-corruptiebeleid moet het net dus breed worden uitgeworpen.

De rol van de auditcommissie

Het is de rol van de auditcommissie om toe te zien of het bestuur corruptierisico's adequaat beheerst en minimaliseert. De auditcommissie zal verder alert zijn op de normen en waarden van de organisatie. Is er sprake van een gezonde, weerbare cultuur? Geeft het bestuur zelf het goede voorbeeld, hoe is de toon aan de top?

Het is ook van belang om de (meldingen op basis van de) klokkenluidersregeling nauwlettend in de gaten te houden: meldingen moeten serieus genomen en opgevolgd worden.

De auditcommissie kan ook Internal Audit vragen een onderzoek te doen en de externe accountant vragen naar diens bevindingen en indrukken tijdens een private session. Zie ook de hoofdstukken 5 (Cultuur en gedrag) en 6 (over de relatie met Internal Audit en de externe accountant).



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's

2. Monitoren van de interne risicobeheersings- en controlesystemen

3. Afstemmen met Internal Audit

4. Afstemmen met de externe accountant

5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht

Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Corruptierisico: waar kan de auditcommissie op letten?

Risicoanalyse: moet alle aspecten van de organisatie dekken, inclusief alle landen waarin deze actief is en alle soorten van activiteiten, en moet worden geactualiseerd bij nieuwe bedrijfsactiviteiten of bij activiteiten in een nieuw geografisch gebied. Maak een **integrity due diligence** een integraal onderdeel van een acquisitie.

Training: moet met name gericht worden op werknemers en relevante derde partijen (zoals agentschappen) in posities die kwetsbaar zijn voor compliance en moet lokaal worden uitgevoerd.

Sancties: het vaststellen, communiceren en afdwingen van de gevolgen bij overtredingen van het beleid.

Monitoren: stel vast dat de juridische afdeling wordt betrokken bij het goedkeuren van het aangaan van relaties met agentschappen en distributeurs.

- Transacties met een hoger risicoprofiel, zoals reis- en verblijfkosten, marketing- en adviesvergoedingen, giften en contributies

aan goede doelen of politieke bijdragen moeten regelmatig worden gereviewed op de grondslag voor betaling. Ook verkoopcommissies en kortingen moeten in dit verband worden gereviewed.

- Overheidscontracten moeten worden geïdentificeerd, en gevolgd.
- Overweeg of de klokkenluidersprocedure toegankelijk moet worden gemaakt voor belangrijke leveranciers en/of derde partijen.
- Bekijk of de organisatie in geval van aanbestedingen van contracten het risico van steekpenningen voldoende mitigeert.
- Evalueer of de organisatie een adequaat due diligence-onderzoek uitvoert met betrekking tot omkopings- en corruptierisico's in het geval van acquisities, overnames en het aangaan van nieuwe contracten met (nieuwe) relaties/ derde partijen.
- Onderzoek of de organisatie haar recht (**right to audit**) uitoefent om de compliance van derde partijen te controleren en compliancecertificaten verkrijgt van leveranciers of derde partijen.
- Stel regelmatig de toereikendheid van de gedragscode vast en verzoek regelmatig om informatie van het bestuur over hoe deze code wordt gecommuniceerd aan de werknemers en aan derde partijen.

8. Fiscale risico's

De auditcommissie houdt volgens de Code toezicht op het fiscale beleid van de organisatie. Dit onderwerp wordt steeds relevanter, gezien de groeiende belangstelling voor belastingen door stakeholders. De moderne samenleving ziet belastingen niet meer alleen als een kostenpost voor de korte termijn, maar als een instrument voor sociaal-economische cohesie, duurzame waardecreatie en welvaart op de lange termijn. Belastingen leveren een belangrijke bijdrage aan duurzame ontwikkeling en langetermijnwaardecreatie voor de organisatie én de maatschappij.

We adviseren de auditcommissie de dialoog met het bestuur aan te gaan over drie belangrijke punten:

1. **het huidige fiscale beleid:** is dit in lijn met maatschappelijke verwachtingen van stakeholders en het ESG-beleid (environment, social and governance) van de organisatie zelf?;
2. **de interne controle en beheersing met betrekking tot de fiscale risico's:** kan de organisatie aantonen dat fiscale risico's worden beheerst en zijn structurele veranderingen in het internationale fiscale landschap in voldoende mate meegenomen?;

3. **transparantie:** op welke manier rapporteren we over fiscaliteit in financiële en niet financiële rapportages, hoe sluit dit aan bij de door de organisatie gebruikte ESG-rapportagestandaarden en vragen we hier externe assurance op?

1. Verantwoord belastingbeleid
Organisaties hebben te maken met een maatschappelijke vraag om een verantwoord en transparant fiscaal beleid. Dit wordt versterkt doordat organisaties zoals de EU, de Organisatie voor Economische Samenwerking en Ontwikkeling, de VN, VN Global Compact, VN Principles for Responsible Investment, het World Economic Forum en het Global Reporting Initiative, de fundamentele rol van belastingen voor duurzame ontwikkeling onderstrepen. Overheden gebruiken belastingopbrengsten om duurzame ontwikkeling, de EU Green Deal en initiatieven voor het tegengaan van klimaatverandering te financieren, maar ook om gedragsverandering te stimuleren (milieu- en klimaatheffingen) en de herverdeling van inkomsten (progressief belastingstelsel).

Passend bij de 'purpose' en ESG-beleid
Steeds meer organisaties formuleren een purpose: een maatschappelijk doel en bestaansrecht. Het ESG-beleid van de organisatie is gekoppeld aan de purpose. Het fiscale beleid sluit aan bij het maatschappelijke doel en vergroot de

- 1. Commissie
 - 2. Continuïteit
 - 3. Corporate impact
 - 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelicht
- Bijlagen

- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

impact van het ESG-beleid. Fiscaliteit is van belang bij alle drie onderdelen van ESG. Op het gebied van environment zijn dit bijvoorbeeld milieubelastingen en subsidies. Voor social kun je denken aan **remuneration, equal pay** en **diversity & inclusion**. Bij governance gaat het om **tone at the top**, fiscale strategie, risicomanagement en transparantierapportage. Zie hiervoor ook afbeelding 1.

Verantwoord fiscaal beleid beschrijft de visie van de organisatie op belastingheffing, verbindt het fiscale gedrag van de organisatie aan het maatschappelijk doel, omvat fiscale criteria, is afgestemd op de duurzaamheidsambities

van de organisatie (ESG) en Sustainable Development Goals (SDG's), beschrijft fiscale controle en beheersing, bevat concrete criteria voor verantwoorde belastingplanning, een visie op fiscale transparantie en meer. Belangrijk is daarnaast dat het beleid systematisch wordt toegepast. Dit houdt in dat het beleid van toepassing is op de gehele organisatie, inclusief de producten, diensten, investeringen, klanten, werknemers en zakenpartners.

De rol van de auditcommissie
De auditcommissie gaat de dialoog aan met het bestuur over het fiscale beleid: hoe fiscaal verantwoord wil de organisatie zich opstellen

en wat is daarvoor nodig? Wat is volgens het bestuur de juiste balans tussen rendement en risico? Wat vinden we vandaag, maar ook morgen nog acceptabel op fiscaal gebied en vinden we hetzelfde als we er morgen extern verantwoording over af moeten leggen? Welke risico's lopen we in de komende jaren? Hoe toekomstbestendig is onze fiscale structuur? Zijn er vormen van belastingontwijking die we voor onze organisatie niet (meer) acceptabel vinden? Welke keuzes en grenzen maakt onze organisatie op fiscaal gebied?

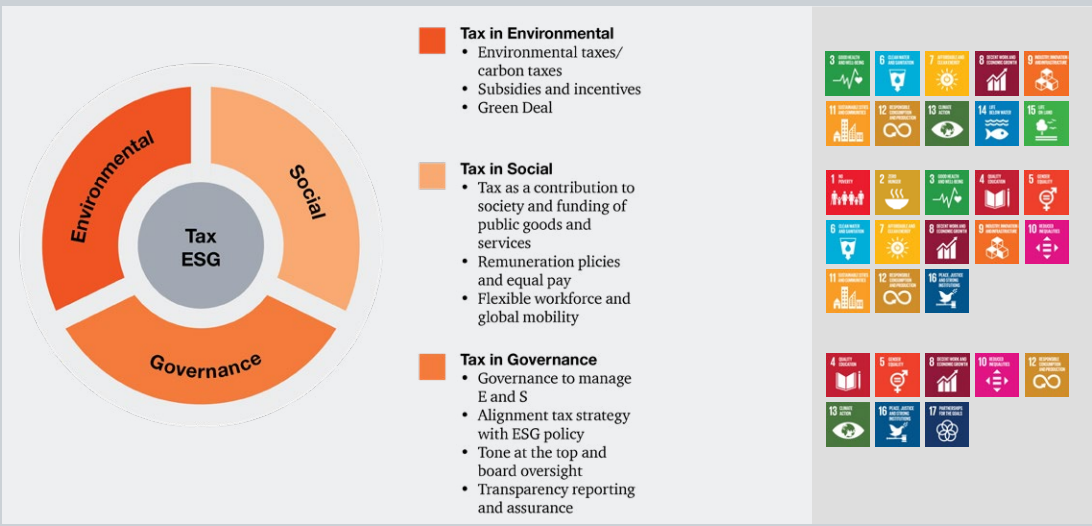
2. Is de organisatie aantoonbaar in control op fiscaal gebied?

Niet alleen het reputatierisico is toegenomen, maar ook het fiscale compliancerisico. De focus in het internationale fiscale landschap is verschoven van reactief naar proactief: van fiscale controle door (externe) toezichthouders, achteraf naar de organisatie die zelf continu aantoonbaar fiscaal in control en compliant moet zijn. Een internationale trend is geregleerde zelfcontrole (in Nederland ook wel aangeduid als Doorontwikkeld Horizontaal Toezicht), ondersteund door automatisering.

Veel landen hanteren het coöperatieve compliancemodel: als organisaties het vertrouwen krijgen van fiscale autoriteiten en het risico op niet-naleving wordt laag ingeschat, dan wordt er minder gecontroleerd door de fiscale autoriteiten. Dat vertrouwen moet wel verdiend en voortdurend aangetoond en bevestigd worden.

We zien een toename in regelgeving, die zich voornamelijk buiten fiscale wetgeving om voltrekt. Naast de traditionele fiscale regels ('deze post is wel of niet aftrekbaar') worden organisaties steeds meer geconfronteerd met **soft law**: gedragscodes, risicobenaderingen, standaarden, principes en richtlijnen. Dat maakt compliance complexer en meer diffuus. Het gaat niet langer om het alleen aan de wet houden, maar ook steeds meer om het daadwerkelijk toepassen van gedragscodes of richtlijnen waarin open normen zijn

Afbeelding 1: Fiscaliteit als onderdeel van ESG



Best practice
Stel als auditcommissie de volgende vraag aan het bestuur en de director Tax:

Zouden we de fiscale structuur van de organisatie ook (blijven) hanteren als we verplicht zouden worden daarover extern verantwoording af te leggen? Hoe toekomstbestendig is onze fiscale structuur? Welke risico's lopen we in de komende jaren?

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

1. Beoordelen van de risico's
 2. Monitoren van de interne risicobeheersings- en controlesystemen
 3. Afstemmen met Internal Audit
 4. Afstemmen met de externe accountant
 5. Interne en externe verantwoording
 6. Enkele risicocategorieën uitgelicht
- Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

opgenomen. Dat vraagt om gedegen governance op belastinggebied. Belangrijk is om hierbij op te merken dat governance betrekking heeft op op alle beloftes gemaakt in het fiscale beleid. Zo moet een principe als “Wij doen niet aan agressieve belastingplanning” concreet worden gemaakt met do's en don'ts en beheerst worden in relevante processen, zoals structurering- of investeringsprocessen. Deze concretisering is niet alleen nodig voor de uitvoering en beheersing, maar ook voor het meten en rapporteren van de fiscale impact.

Internationale hefboom

De auditcommissie ziet erop toe dat de organisatie fiscaal aantoonbaar in control is. Als de interne controle op orde is, kan dat functioneren als een hefboom voor de relatie met de fiscale autoriteiten in alle landen waarin de organisatie actief is. Wanneer er vertrouwen is in de fiscale beheersing (het ‘tax control framework’), zal minder worden gecontroleerd door deze autoriteiten.

■ De rol van de auditcommissie

De auditcommissie houdt toezicht op de risicobeheersings- en controlesystemen op het gebied van fiscaliteit. Hoe effectief is bijvoorbeeld het interne validatiesysteem voor de juistheid en volledigheid van de belastingaangifte? Hoe worden fiscale risico's geïdentificeerd en gemonitord?

In hoeverre wordt soft law meegenomen? Welke belastingen worden meegenomen (niet alleen vennootschapsbelasting, maar ook omzetbelasting, loonbelasting, heffingen en accijnzen, milieubelastingen, et cetera)? Hoe gaat de organisatie om met het witwasrisico (belastingontduiking) en is er sprake van naleving van wet- en regelgeving op dat gebied? Is het tax control framework een geheel van de identificatie van fiscale risico's en de interne beheersing, interne controle en externe controle van deze fiscale risico's? Hoe en wanneer wordt beoordeeld wat de effectiviteit is van het tax control framework? Op welke manier is Internal Audit hierbij betrokken?

Welke mensen hebben we nodig voor goede fiscale governance en hebben we deze mensen in huis? Zijn de fiscale systemen volledig geïntegreerd in de financiële rapportagesystemen? Beschikken we over een sterk en veilig ondersteunend technologisch platform? Is de organisatie bereid tot externe tax assurance: een door een externe accountant afgegeven verklaring aan de stakeholders dat de organisatie fiscaal in control is in brede zin (dus ook in ethisch-moreel opzicht)?

3. Transparantie

Fiscale transparantie vormt het sluitstuk van een verantwoord fiscaal beleid. Door transparant over fiscaliteit te rapporteren, financieel en niet financieel, kan een organisatie verantwoording afleggen aan de stakeholders over de uitvoering en impact van het belastingbeleid. Het is daarbij van belang om te bepalen wat de maatschappelijke verwachtingen zijn op het gebied van fiscale transparantie. Veelal wordt gevraagd om transparantie over de fiscale strategie, inclusief stakeholderengagement, governance, risicomanagement, en country by country reporting (belastingafdracht per jurisdictie).

Een standaard die deze verwachtingen samenvat is de fiscale transparantiestandaard van Global Reporting Initiative, (GRI 207: Tax 2019). Deze standaard is tot stand gekomen met input van vele stakeholders en wordt door diverse organisaties gebruikt voor externe transparantie en rapportage over fiscaliteit. Accountants kunnen non-financial assurance geven op deze rapportage.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

- 1. Beoordelen van de risico's
- 2. Monitoren van de interne risicobeheersings- en controlesystemen
- 3. Afstemmen met Internal Audit
- 4. Afstemmen met de externe accountant
- 5. Interne en externe verantwoording

6. Enkele risicocategorieën uitgelicht
Bijlagen

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

■ De rol van de auditcommissie

De auditcommissie gaat het gesprek aan met het bestuur over fiscale transparantie. Hierbij is het accent verschoven van **tell me** naar **show me** en **prove me**. Hoe rapporteren we aan onze interne en externe stakeholders over de implementatie en uitvoering van ons fiscale beleid? Op welke manier rapporteren we over eventuele fiscale risico's, waaronder financiële, wetgevings- en/of reputatierisico's? Rapporteren we over fiscale overeenkomsten (rulings) die worden afgesloten met fiscale autoriteiten en welke informatie publiceren we? Wat moet er nog gebeuren om een accountant te kunnen vragen een verklaring af te geven op de fiscale informatie die bijvoorbeeld wordt gepubliceerd in het kader van de GRI 207? Zie bijlage 4A.

Uit de praktijk

Voorbeeld transparantie over belastingen in bestuursverslag

De Tax Transparency Benchmark is een onderzoek uitgevoerd door de Vereniging van Beleggers voor Duurzame Ontwikkeling (VBDO) dat kijkt naar de belastingtransparantiepraktijken van Nederlandse en Europese beursgenoteerde bedrijven. In 2023 beoordeelde de benchmark 51 Nederlandse bedrijven en 65 beursgenoteerde bedrijven uit België, Denemarken, Frankrijk, Duitsland, Italië, Spanje en Zweden. Deze bedrijven opereren in verschillende sectoren zoals financiën, energie, farmaceutica, technologie en consumentengoederen.

Philips is uitgeroepen tot het meest transparante bedrijf op het gebied van belastingafdracht volgens de Tax Transparency Benchmark 2023. Het gezondheidstechnologiebedrijf behaalde een perfecte score in elke categorie van de benchmark met een totaalscore van veertig punten, een unicum in de geschiedenis van de benchmark. De jury was vooral onder de indruk van de diepgang en kwaliteit van het belastingverslag van Philips. Philips' belastingaanpak is een integraal onderdeel van hun Environmental, Social, and Governance (ESG)-verplichtingen. In 2022 behaalde Philips nog 32 punten, en een jaar eerder 31 punten. De jury waardeerde de uitgebreide landenrapportage van Philips, expliciet gekoppeld aan de GRI 207 Tax Standard, en informatie over milieu- en sociale factoren. Daarnaast prees de jury Philips voor de duidelijke beschrijving van de rol die belastingen spelen binnen hun waardecreatiemodel.



Best practices voor de auditcommissie

- Worden de fiscale uitgangspunten van de top ook in de financiële kolom en de internationale vestigingen gedeeld? Wordt het belastingbeleid in de gehele organisatie nageleefd, of is het een papieren tijger? Vraag Internal Audit om de cultuur en naleving te monitoren.
- Bevraag de ceo en de cfo niet alleen over vennootschapsbelasting, maar ook over indirecte belastingen, zoals loofheffing of energieheffing. Bestuurders zien indirecte belastingen vaak over het hoofd, terwijl ze tot grote fiscale risico's kunnen leiden. Vraag Internal Audit de beheersing van deze risico's in kaart te brengen en te monitoren.
- Welke materialiteit hanteert het bestuur in zijn beoordeling van de fiscale positie en het in control zijn van de organisatie rondom fiscaliteit? Sluit die materialiteit aan bij de door de Nederlandse belastingdienst en buitenlandse belastingdiensten gehanteerde materialiteit?

Bijlagen

Bijlage 4A

GRI 207: Tax 2019 High level overview of reporting requirements

Bijlage 4A GRI 207: Tax 2019

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
 - 1. Beoordelen van de risico's
 - 2. Monitoren van de interne risicobeheersings- en controlesystemen
 - 3. Afstemmen met Internal Audit
 - 4. Afstemmen met de externe accountant
 - 5. Interne en externe verantwoording
 - 6. Enkele risicocategorieën uitgelichtBijlagen
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

High level overview of reporting requirements

1 Approach to tax	2 Tax governance, control and risk management	3 Stakeholder engagement and management concerns	3 Country by country reporting/ Tax-Contribution reporting
• Tax strategy • Governance body that formally reviews and approves the tax strategy • Approach to compliance • Link to the business and sustainable development strategies	• Governance body accountable for compliance with the tax strategy • How the approach to tax is embedded in the organisation • Risk management • Mechanisms for reporting concerns • Assurance process	• Approach to engagement with tax authorities • Approach to public policy advocacy • Stakeholders engagement	• Country by country reporting data • Total tax contribution data
			



Cultuur en gedrag

Voorkomen misstanden en onregelmatigheden: soft controls

05

5. Cultuur en gedrag

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de **purpose** en de kernwaarden
 - 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
 - 3. Meten en monitoren van cultuur en gedrag
 - 4. Toetsen van de gedragscode
 - 5. Voorkomen misstanden en onregelmatigheden
 - 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Een gezonde organisatiecultuur creëert verbondenheid in een turbulente omgeving, is gericht op langetermijnwaardecreatie en kan misstanden en onregelmatigheden helpen voorkomen. De raad van commissarissen houdt toezicht op cultuur en gedrag. De auditcommissie kan de raad van commissarissen daarbij ondersteunen door het monitoren van cultuur(verandering) en het vroegtijdig signaleren en beperken van de risico's die daaraan zijn verbonden.

Cultuur bestaat uit de collectieve normen en waarden, resulterend in gemeenschappelijk gedrag binnen de organisatie. Die normen en waarden vormen een referentiekader op basis waarvan het eigen handelen en dat van anderen wordt beoordeeld: wie zijn we als organisatie, waar staan we voor en hoe doen we de dingen? Cultuur is de gedeelde en vaak impliciete context waarin de medewerkers van de organisatie opereren, **'the smell of the place'**.

Verbondenheid in tijden van verandering

Een sterke en gezonde cultuur creëert saamhorigheid in de organisatie. Die onderlinge verbondenheid zorgt voor robuustheid bij turbulentie: de gemeenschappelijke normen en waarden vormen een vaste basis in een voortdurend veranderende omgeving. Dat geeft houvast, maar zorgt er tegelijkertijd voor dat de organisatie juist durft los te laten en flexibel weet in te spelen op verandering. De normen en waarden zelf veranderen niet, maar de invulling ervan ademt mee met de ontwikkelingen. Dat

Er is geen one-size-fits-allcultuur. Wat sterk is in de cultuur van de ene organisatie (bijvoorbeeld een focus op regels, (veiligheids)procedures en handhaving in een risicovolle technische omgeving) kan zwak zijn in de cultuur van een andere organisatie (zoals een startup, waar het accent juist ligt op kernwaarden als flexibiliteit en klantgerichtheid en veel informeel overleg om de markt te veroveren en snel in te spelen op kansen).

adaptieve vermogen vormt een belangrijke overlevingsfactor in disruptieve tijden. Een sterke en gezonde cultuur is bovendien gericht op langetermijnwaardecreatie en ondersteunt daarmee het realiseren van de strategische doelstellingen. Cultuur en gedrag zijn dan ook bepalend voor de toekomstbestendigheid en daarmee voor de continuïteit van organisaties.

In dit hoofdstuk komen de volgende onderwerpen aan de orde:

1. Toezicht op purpose en kernwaarden
2. Toetsen gewenste cultuur versus werkelijke cultuur
3. Meten en monitoren van cultuur en gedrag
4. Toetsen gedragscode
5. Voorkomen misstanden en onregelmatigheden
6. Verantwoording afleggen over cultuur en gedrag



Houvast en vertrouwen

Intern biedt een sterke en gezonde cultuur managers en medewerkers houvast voor het dagelijkse gedrag en het omgaan met dilemma's. Extern kan zo'n cultuur – en als onderdeel daarvan integer gedrag – bijdragen aan het vertrouwen van stakeholders en een voorwaarde vormen voor een goede positie op de arbeidsmarkt en voor samenwerking in de keten. (Potentiële) medewerkers, klanten, leveranciers en aanbestedende overheden kijken in toenemende mate naar normen en waarden bij de selectie van organisaties waarvoor en waarmee ze willen werken. Een gezonde cultuur is ook essentieel voor een maatschappelijke **license to operate**.

Kenmerken van een sterke en gezonde cultuur:

- intern en extern is duidelijk waar de organisatie voor staat;
- alle medewerkers in de organisatie weten hoe zij bijdragen aan het hogere doel, de verwachtingen van stakeholders en het resultaat;
- er is duidelijkheid over structuur, rollen en verantwoordelijkheden;
- er zijn heldere afspraken over wat constructief gedrag is en wat niet;
- managers en medewerkers spreken elkaar aan op ongewenst gedrag;
- de organisatie is in staat effectief in te spelen op verandering.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

1. Toezicht op de **purpose** en de kernwaarden
2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
3. Meten en monitoren van cultuur en gedrag
4. Toetsen van de gedragscode
5. Voorkomen misstanden en onregelmatigheden
6. Verantwoording afleggen over cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Risico voor continuïteit?

Andersom kunnen een ongezonde cultuur en ongewenst gedrag het vertrouwen en de reputatie schaden en daarmee de continuïteit van de organisatie bedreigen. Cultuur en gedrag zijn idealiter dan ook volledig geïntegreerd in de risicobeheersing en interne controle. Het gaat bij risicobeheer immers niet alleen om naleving van wet- en regelgeving, adequate systemen voor interne controle en beheersing, heldere procedures en richtlijnen, duidelijke verantwoordelijkheden en het afleggen van verantwoording (**hard controls**), maar ook om de menselijke factor: waarden en normen, de daadwerkelijke beleving en toepassing daarvan in de praktijk en elkaar aanspreken op gedrag (**soft controls**).

Ongrijpbaar fenomeen?

De belangrijkste rol van de raad van commissarissen is het waarborgen van de continuïteit van de organisatie. Goed (toe)zicht op cultuur en gedrag is daarbij essentieel. Dat is gemakkelijker gezegd dan gedaan, want hoe krijg je als toezichthouders grip op deze ‘zachte’ factoren? Hoe geef je handen en voeten aan het toezicht op een ‘ongrijpbaar fenomeen’ als cultuur? Welke vragen moet je daarover stellen? Hoe krijg je concrete informatie over cultuur en gedrag boven tafel? Op welke signalen moet je letten, hoe leg je contact met interne en externe stakeholders en hoe houd je voeling met wat er binnen en buiten de organisatie gebeurt?



Kernvragen voor het toezicht op cultuur en gedrag

1. Worden cultuur en gedrag gezien als strategisch belangrijk op het niveau van het bestuur?
2. Is er een centraal waardensysteem, dat is vertaald in voorbeeldgedrag, symbolen en besluitvorming en processen, systemen en procedures?
3. Weten mensen op alle niveaus binnen de organisatie hoe ze moeten handelen en voelen ze zich verantwoordelijk voor hun gedrag?
4. Is essentieel gedrag op ‘momenten van de waarheid’ (kritische beslissingen en interactie met stakeholders, die bepalend zijn voor de externe perceptie en reputatie) duidelijk omschreven en afgestemd op het doel, de visie en het waardensysteem?
5. Beseffen succesvolle organisaties dat waardegedreven leiderschap op alle niveaus doorwerkt: **tone at the top, in the middle and from the tail**?
6. Zitten alle medewerkers op één lijn en is er geen verschil tussen het gewenste en het werkelijke gedrag? Is het gedrag meetbaar en bespreekbaar?

■ De rol van de auditcommissie

Concretiseren en monitoren

De auditcommissie ziet toe op een juiste interne beheersing en speelt daarmee een belangrijke voorbereidende rol in de ondersteuning van de raad van commissarissen. Een belangrijk onderdeel van interne beheersing is cultuur en gedrag, inclusief de toon aan de top. Het is de rol van de auditcommissie het toezicht op cultuur en gedrag zo concreet mogelijk te maken, zorgvuldig te monitoren en daarvan regelmatig verslag te doen aan de overige commissarissen. De rol van de auditcommissie vloeit logisch voort uit de taken van de auditcommissie op het gebied van de interne controle en beheersing, waarbij zowel gekeken moet worden naar **hard controls** als naar **soft controls**. Bovendien ziet de auditcommissie toe op het gehele spectrum aan risico's voor de organisatie. Dat omvat ook cultuur- en integriteitsrisico's. Zie hiervoor ook hoofdstuk 4 over risicobeheer en interne controle.

Purpose en kernwaarden als vertrekpunt

Toezicht op cultuur en gedrag mag zich echter niet beperken tot technische en materiële maatregelen op het gebied van interne beheersing en controle, om het risico op ongewenst gedrag in de organisatie te beperken. Regels alleen kunnen integriteitsproblemen niet voorkomen, of gevoel voor maatschappelijke verhoudingen afdwingen. Het hogere doel – de **purpose** – en de daarvan afgeleide kernwaarden fungeren als vertrekpunt voor het toezicht op cultuur en gedrag: wie zijn we als organisatie, waar staan we voor en hoe

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

- 1. Toezicht op de **purpose** en de kernwaarden
- 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
- 3. Meten en monitoren van cultuur en gedrag
- 4. Toetsen van de gedragscode
- 5. Voorkomen misstanden en onregelmatigheden
- 6. Verantwoording afleggen over cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

doen we de dingen? Is er sprake van een sterke en gezonde cultuur, die verbondenheid in de organisatie creëert? Dat werken we in het vervolg van deze publicatie verder uit.

Toon aan de top

Het gaat bij cultuur en gedrag niet alleen om de waarden en normen in de organisatie, maar ook om die in de bestuurskamer. Wat zien bestuurders en commissarissen als de **purpose** van de organisatie, welk moreel kompas hanteren ze bij het realiseren daarvan, hoe gaan ze daarbij om met de belangen van stakeholders en hoe integer zijn ze in hun denken en handelen? Kortom: hoe is de toon aan de top?

Dynamiek in de bestuurskamer

Als we het hebben over cultuur in de bestuurskamer, kan dat ook betrekking hebben op de dynamiek binnen en tussen het bestuur en de raad van commissarissen: is er sprake van vertrouwen of wantrouwen, is er ruimte voor tegenspraak en kritische toetsing, is er bewustzijn van en alertheid op gevaren als tunnelvisie en

groupthink? De voorzitter en de leden van de auditcommissie moeten zich bewust zijn van die dynamiek en vooringenomenheid: in de eigen commissie, in de relatie met het bestuur/de cfo en met de rest van de commissarissen. De Code stelt dat het bestuur en de raad van commissarissen elk verantwoordelijk zijn ‘voor het stimuleren van openheid en aanspreekbaarheid’ binnen het eigen orgaan en tussen de gremia onderling. Dat geldt natuurlijk ook voor de auditcommissie.

Diversiteit nodig in samenstelling auditcommissie

Bij de selectie en **onboarding** van nieuwe leden van de auditcommissie is het goed om uitgebreid aandacht te besteden aan de gewenste cultuur in de auditcommissie en de gedragsmatige aspecten die daarin een rol spelen. Diversiteit kan hieraan een positieve impuls geven. Het is verstandig om ook bij de samenstelling van de auditcommissie te streven naar diversiteit in brede zin, bijvoorbeeld op het gebied van geslacht, leeftijd, achtergrond en persoonlijkheid. Zie hiervoor ook hoofdstuk 1, waarin de opzet en het functioneren van de auditcommissie wordt besproken.

Best practice

Een zwak ontwikkeld normbesef aan de top beïnvloedt de opstelling van medewerkers in de gehele organisatie.
De auditcommissie neemt de toon aan de top dan ook nadrukkelijk mee in de analyse en monitoring van de cultuur.



1. Toezien op de purpose en de kernwaarden

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de purpose en de kernwaarden
 - 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
 - 3. Meten en monitoren van cultuur en gedrag
 - 4. Toetsen van de gedragscode
 - 5. Voorkomen misstanden en onregelmatigheden
 - 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Cultuur vormt ook een van de pijlers in de Code. Het bestuur is volgens de Code verantwoordelijk voor het vormgeven van een cultuur die is gericht op langetermijnwaardecreatie; de raad van commissarissen houdt daarop toezicht. De Code schrijft niet voor wat cultuur precies is of zou moeten zijn. Het is de verantwoordelijkheid en taak van het bestuur om daaraan zélf een organisatie-specifieke invulling te geven.

Het bestuur stelt volgens de Code daarbij de waarden vast en bespreekt deze met de raad van commissarissen. Waarden en cultuur moeten zijn gericht op langetermijnwaardecreatie en ondersteunend zijn aan het bedrijfsmodel en de strategie, rekening houdend met de (maatschappelijke) omgeving waarin de organisatie opereert.

Actieve inbreng raad van commissarissen gewenst

De Code stelt niet dat het bestuur de raad van commissarissen bij dit proces betreft (zoals wel ten aanzien van strategie gesteld wordt), terwijl een actieve inbreng van de raad van commissarissen bij een belangrijk thema als cultuur en het vaststellen van de kernwaarden wel zeer gewenst is. De kernwaarden vloeien direct voort uit de **purpose**: het hogere doel en het maatschappelijk bestaansrecht van de organisatie. Ze vormen een concrete verwoording van : de ongeschreven regels en impliciete normen en waarden. Explicitering daarvan in kernwaarden vormt een moreel ijkpunt en richtsnoer voor het dagelijks handelen. Het bestuur stelt de kernwaarden vast, maar kan dat

niet alleen. Essentieel bij het vaststellen van de kernwaarden is het voeren van een dialoog over de gedeelde normen en waarden met alle medewerkers en externe stakeholders. Als de kernwaarden worden opgelegd door de top, zullen ze niet worden omarmd door de organisatie.

De rol van de auditcommissie

Vanuit haar toezichtrol kan de auditcommissie een belangrijke bijdrage leveren aan de discussie met het bestuur (of de raad van commissarissen daarin ondersteunen) ten aanzien van de gewenste cultuur en de formulering van de kernwaarden. De auditcommissie is immers verantwoordelijk voor de beoordeling van de risico's van het businessmodel voor de continuïteit op korte en lange termijn

en voor een zorgvuldige monitoring van het waardecreatieproces en de executie van de strategie. De auditcommissie zal dan ook mede vanuit haar verantwoordelijkheid voor risicomanagement reflecteren op de cultuur en de kernwaarden die het bestuur wil vormgeven en heeft vastgesteld, vanuit de **purpose** van de organisatie en de belangen van alle stakeholders.

De auditcommissie ziet ook toe op het proces rond de formulering van de kernwaarden. Voert het bestuur daartoe een dialoog met de organisatie, zodat de kernwaarden breed gedragen worden? De auditcommissie heeft vervolgens de taak om zorgvuldig te analyseren en monitoren in hoeverre de cultuur zich in de gewenste richting ontwikkelt

Best practice voor sturen en toezien op cultuur volgens de Nederlandse Corporate Governance Code

Het bestuur stelt voor de organisatie waarden vast die bijdragen aan een cultuur gericht op langetermijnwaardecreatie en bespreekt deze met de raad van commissarissen. Het bestuur is verantwoordelijk voor de inbedding en het onderhouden van de waarden in de onderneming. Daarbij wordt onder meer aandacht besteed aan:

- de strategie en het bedrijfsmodel;
- de omgeving waarin de onderneming opereert; en
- de bestaande cultuur binnen de onderneming en of het gewenst is daar wijzigingen in aan te brengen.

Het bestuur stimuleert gedrag dat aansluit bij de waarden en draagt deze waarden uit door het tonen van voorbeeldgedrag. Dit voorbeeldgedrag moet zijn gebaseerd op de gewenste cultuur en niet op de werkelijke cultuur, die immers juist moet veranderen.

Subculturen verbinden door centrale waarden

In de meeste organisaties is sprake van verschillende subculturen. Eenvoudige voorbeelden zijn de specifieke culturen van de 'lijn', de 'staven' en de 'bazen'. Die subculturen zijn nodig om mensen het gevoel te geven ergens bij te horen in de organisatie en beter te laten functioneren. In internationale organisaties vormen ook de landenvestigingen vaak subculturen, ontstaan door de geografische afstand tussen de buitenlandse dochterorganisaties en het hoofdkantoor en door de nationale cultuur van de verschillende landen waarin wordt geopereerd. Ondanks de verschillen is het belangrijk dat al deze subculturen zich verbonden voelen door dezelfde kernwaarden.

en de kernwaarden worden gehanteerd als richtsnoer voor het gedrag in de praktijk.

Rekening houden met cultuurverschillen binnen de organisatie

Bij het vormgeven van cultuur moet volgens de Code rekening worden gehouden met het bestaan van verschillende subculturen binnen de onderneming: worden de kernwaarden ook daar (h)erkend, geaccepteerd en beleefd als richtsnoer voor dagelijks handelen?

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de **purpose** en de kernwaarden
 - 2. Toetsen van de **gewenste cultuur** versus de **werkelijke cultuur**
 - 3. Meten en monitoren van cultuur en gedrag
 - 4. Toetsen van de gedragscode
 - 5. Voorkomen misstanden en onregelmatigheden
 - 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

2. Toetsen van de gewenste cultuur aan werkelijke cultuur

Het mag bij de formulering van de kernwaarden niet alleen gaan om mooie woorden, het moet vooral gaan om daden: doen wat je zegt, **walk the talk**. **Talk** zonder **walk** werkt averechts. Dat gedrag wordt snel doorgeprikt door interne en externe stakeholders.

Drie dimensies van cultuur en gedrag
Essentieel voor toezicht op cultuur door de raad van commissarissen is dan ook de vraag naar het verschil tussen de gewenste cultuur en het bijbehorende gedrag. Het antwoord kan worden vergeleken met de werkelijke situatie: hoe diep is de kloof tussen de gedefinieerde normen en waarden en het in praktijk brengen daarvan? Ook de Code verlangt dat aandacht wordt besteed aan de vraag of de bestaande cultuur wijzigingen behoeft. Daarvoor kan gekeken worden naar drie dimensies:

- het **voorbeeldgedrag** van de leiders in de organisatie, afgeleid van de **purpose** en de kernwaarden (**Soul**) (voorbeeldgedrag wordt ook expliciet genoemd in de Code);
- het inrichten van **processen, structuren en systemen**, zoals belonings- en benoemingsbeleid (**System**);
- de gehanteerde **symbolen en genomen beslissingen** (**Stamina**).

Dialogo over inbedding waarden
Het is aan de gehele raad van commissarissen om een dialoog met het bestuur te voeren over het verschil tussen de gewenste en de werkelijke cultuur en de inbedding en het onderhoud van waarden daarbij. Bijvoorbeeld door naast de behaalde

Drie dimensies van cultuur en gedrag

Soul
Het **Bezielen** van medewerkers vanuit geloof in (het belang van) de kernwaarden en de eigen identiteit voor de noodzakelijk geachte cultuurverandering.

System
Het **Aantonen** en faciliteren van de cultuurverandering middels systemen, processen en structuren van de organisatie (zoals de organisatiestructuur, het performancemanagement, de beloningssystematiek en de interne controles)

Stamina
Het bestendig **Verankeren** van de cultuur door het sturen op de kernwaarden in de dagelijkse besluitvoering en bedrijfsvoering

resultaten (het ‘wat’) ook te vragen naar de manier waarop die zijn bereikt (het ‘hoe’).

■ **De rol van de auditcommissie**

Toets op integratie cultuur in waardecreatieproces en bedrijfsvoering
De auditcommissie kan de raad van commissarissen ondersteunen bij de dialoog met het bestuur en deze van ‘munitie’ voorzien door met behulp van de drie dimensies te toetsen of de gewenste cultuur volledig geïntegreerd

is in het waardecreatieproces en de dagelijkse bedrijfsvoering. (Zie voorbeeldvragen in het kader op de volgende pagina.)

Best practice
Stel de vraag: klinken de waarden door in elke strategische keuze, investeringsbeslissing, overname of productinnovatie?

Kenmerken van een gezonde cultuur
In een gezonde cultuur valt de **walk** samen met de **talk** en is er sprake van een samenhangende context waarin mensen gestimuleerd worden het goede gedrag te vertonen. Medewerkers durven elkaar aan te spreken op gedrag dat niet in lijn is met de kernwaarden. Dilemma’s zijn bespreekbaar en fouten worden niet verzwegen en afgestraft, maar open en eerlijk gemeld en gezien als waardevolle leerervaring.

Een toepassing hiervan kan zijn dat het melden van fouten wordt gezien en ook benoemd als scherp en alert zijn. De aandacht dient te liggen op de fout of het incident, niet op de persoon. Het erkennen van ‘bijna’-fouten door bestuursleden is eveneens waardevol, ook de fouten die geen of beperkte impact hadden. Wanneer er een open, veilige en diepgaande communicatie is ten aanzien van fouten ontstaat het grootste leereffect. Het formuleren van leerpunten en het delen daarvan binnen de organisatie draagt daaraan bij. Ook het faciliteren van het meelopen in projecten van andere afdelingen stimuleert om van elkaar te leren.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

- 1. Toezicht op de **purpose** en de kernwaarden
- 2. **Toetsen van de gewenste cultuur versus de werkelijke cultuur**
- 3. Meten en monitoren van cultuur en gedrag
- 4. Toetsen van de gedragscode
- 5. Voorkomen misstanden en onregelmatigheden
- 6. Verantwoording afleggen over cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie



Beloningsstructuur als spiegel van de cultuur

Het remuneratiebeleid weerspiegelt de cultuur van de organisatie. Het geeft aan welk gedrag gewaardeerd en (letterlijk) beloond wordt (bijvoorbeeld met een salarisverhoging of bonus) en welk gedrag juist niet gewaardeerd en zelfs ‘bestraft’ wordt (door geen salarisverhoging toe te kennen of bonus uit te keren). De beloningssystematiek maakt duidelijk of de geformuleerde waarden slechts mooie woorden zijn, of daadwerkelijk zijn ingebed in de bedrijfsvoering. Is de beloningssystematiek bijvoorbeeld in lijn met de langetermijndoelstellingen en duurzaamheid van de organisatie, of bevat deze perverse prikkels die uitlokken tot kortetermijngedrag? Daarnaast dient het beloningsbeleid rekening te houden met de identiteit, missie en waarden van de organisatie naast de interne beloningsverhoudingen.

De rol van de auditcommissie

Perverse prikkels voorkomen

Het toekennen van de beloning is een verantwoordelijkheid van de gehele raad van commissarissen. Daarbinnen is het beloningsbeleid het specifieke aandachtspunt van de remuneratiecommissie. Toch ligt hier ook een rol voor de auditcommissie: het toezien op een evenwichtige beloningscultuur die het gewenste gedrag stimuleert en ongewenst gedrag sanctioneert. De beloningsstructuur van zowel bestuurders als werknemers kan zich namelijk ontwikkelen tot een risico, zoals de Code expliciet aangeeft. Perverse prikkels in de beloning kunnen niet alleen leiden tot kortetermijngericht gedrag en daarmee de realisering van de langetermijnstrategie frustreren, maar ook de integriteit van medewerkers en die van de financiële verslaggeving bedreigen, zoals de boekhoudschandalen hebben laten zien. Dat brengt risico’s voor de reputatie en continuïteit met zich mee. Het bestuur moet deze risico’s identificeren en beheersen, de auditcommissie ziet erop toe dat deze risico’s worden gemitigeerd door de (andere) inrichting van

de beloningsstructuur. Dat vraagt om nauwe samenwerking tussen de auditcommissie en de remuneratiecommissie. Dat kan bijvoorbeeld bereikt worden met een dubbellidmaatschap van auditcommissie en remuneratiecommissie en overleg tussen de voorzitters van beide commissies.

Niet alleen ‘wat’, maar ook ‘hoe’ belonen

Een cultuur die is gericht op langetermijnwaardecreatie vraagt om een beloningsstructuur met een gepaste verhouding tussen vaste en variabele elementen. Toekenning van de beloning moet niet alleen plaatsvinden op basis van kwantitatieve, maar ook kwalitatieve, niet-financiële prestatiecriteria. Het gaat niet zozeer om de absolute hoogte van de remuneratie (hoewel ook die moet passen bij de cultuur van de organisatie en de maatschappelijke omgeving waarin deze opereert en de maatschappelijke verantwoordelijkheid die hierin genomen dient te worden), maar om de aansluiting met de identiteit, missie en waarden van de organisatie. Niet alleen het ‘wat’, maar ook het ‘hoe’ moet worden beloond. Deze uitwerking dient sinds 2019 op basis van wettelijke bepalingen in het remuneratiebeleid en het jaarlijkse beloningsverslag gepresenteerd te worden voor elke individuele bestuurder.

Bonus onthouden bij ongewenst gedrag

Zo kunnen bestuurders worden gestimuleerd om ook de belangen van bijvoorbeeld klanten, medewerkers en andere stakeholders te behartigen. Op die basis kan ook de rest van het loongebouw in de organisatie worden opgetrokken. Commissarissen kunnen de beloning ook inzetten om een duidelijk signaal af te geven naar het bestuur, de rest van de organisatie en zelfs de buitenwereld. Bijvoorbeeld door het bestuur een bonus te onthouden bij ongewenst gedrag.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de **purpose** en de kernwaarden
 - 2. **Toetsen van de gewenste cultuur versus de werkelijke cultuur**
 - 3. Meten en monitoren van cultuur en gedrag
 - 4. Toetsen van de gedragscode
 - 5. Voorkomen misstanden en onregelmatigheden
 - 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie



Hoe sterk is de cultuur?

Checklist voor een snelle toets



Voorbeeldgedrag

- Zijn de **purpose** en de waarden van de organisatie duidelijk?
- Is voor iedereen duidelijk wie de externe stakeholders zijn en wat voor hen belangrijk is?
- Wie zijn de rolmodellen binnen de organisatie? Hoe gaat men formeel en informeel met elkaar om?
- Zijn de leiders levende voorbeelden van **purpose** en de waarden van de organisatie?
- Is er bezieling? Is er verbinding? Is er transparantie? Waar blijkt dat uit?
- Worden genomen besluiten ook uitgevoerd? Is afspraak ook afspraak?
- Hoe zorg je voor samenhang en een gedeeld waardenbesef in de gehele organisatie? Versterken of verzwakken de subculturen binnen de organisatie de omslag naar de gewenste cultuur?
- Gelden er voor leiders en hun **inner circles** afwijkende spelregels of bijzondere privileges: hebben ze het gevoel 'onder en boven de wet' te staan?
- Staan de leiders open voor kritiek en het beantwoorden van vragen?
- Wat gebeurt er als er fouten gemaakt worden? Hoe leert de organisatie?



Symbolen en beslissingen

- Hoe zorgt de organisatie dat leiders in overeenstemming handelen met de **purpose** en de waarden?
- Welke waarden hebben echt waarde?
- Hoe blijkt dit uit het leiderschap? Wat krijgt prioriteit? Welk punt valt altijd van de agenda?
- Wordt diversiteit bewaakt (m/v en multiculturele aspecten)?
- Hoe werken performancereviews? Hoe worden mensen beoordeeld? Hoe worden mensen beloond of gestraft voor het al dan niet bijdragen aan de **purpose** en de waarden? Hoe ver gaat de organisatie daarin?
- Hoe nemen we moeilijke besluiten? Hoe gaan we om met dilemma's? Zijn we hier transparant over naar alle stakeholders?
- En ook platter: Wie parkeert waar? Wie zit in welk kantoor? Wie neemt deel aan de leukste uitjes en reisesjes?



Structuren en systemen

- Is de organisatiestructuur en de inrichting in lijn met de **purpose** en de waarden van de organisatie?
- Waar liggen de verantwoordelijkheden? Welke autorisaties liggen waar en zijn de limieten duidelijk?
- Hoe ziet de planning en de budgettering er uit? Hoe ziet de managementinformatie er uit?
- Wat wordt er feitelijk gemeten? Waarover wordt gerapporteerd?
- Hoe ziet risicobeheer eruit? Is er een compliancefunctie? Hoe werkt de interne controle?
- Wat staat er in de regels en codes? Is er een klokkenluidersregeling?
- Handelen de ondersteunende functies als één in het belang van de organisatie?
- Zijn de ondersteunende functies een volwaardig gesprekspartner voor de business?

3. Meten en monitoren van cultuur en gedrag

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de **purpose** en de kernwaarden
 - 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
 - 3. **Meten en monitoren van cultuur en gedrag**
 - 4. Toetsen van de gedragscode
 - 5. Voorkomen misstanden en onregelmatigheden
 - 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Organisaties kunnen meer grip krijgen op cultuur en gedrag door deze goed in beeld te brengen, voor zover mogelijk meetbaar te maken en zorgvuldig te monitoren. Dat vraagt om een afgewogen mix van zowel **hard controls** als **soft controls**. Zo kan de organisatie een dashboard ontwikkelen met niet alleen kpi's, maar ook kbi's (**key behavioral indicators**), afgeleid van de kernwaarden en de gedragsaspecten waarop de organisatie wil sturen. Daartoe worden cultuur en gedrag concreet vertaald naar de dagelijkse praktijk zodat medewerkers weten welk gedrag er van hen verwacht wordt, binnen welke kaders ze zich bij de uitoefening van hun functie kunnen bewegen en welke grenzen niet overschreden mogen worden.

Zo nodig bijsturen
Kbi's geven de mate aan waarin medewerkers het gewenste gedrag vertonen. Op die manier kan vroegtijdig signaleerd worden of de werkelijke cultuur afwijkt van de gewenste cultuur en kan eventueel worden bijgestuurd. Volgens de Code wordt het bestuur geacht de werking van de

Best practice

Stel de vraag: is duidelijk hoe medewerkers zich dienen te gedragen en welke grenzen niet mogen worden overschreden? Hoe meer duidelijkheid over (on)gewenst gedrag, hoe sterker en effectiever de werking van cultuur als **soft control**.

interne risicobeheersings- en controlesystemen te monitoren en ten minste jaarlijks een systematische beoordeling uit te voeren van de opzet en de werking van de systemen. Als dat voor de **hard controls** geldt, waarom dan niet ook voor de **soft controls**?

De rol van de auditcommissie
Cultuur en gedrag agenderen en monitoren
De auditcommissie vraagt aan het bestuur hoe cultuur en gedrag gemonitord worden en hoe daarover inhoudelijk wordt gerapporteerd. Om een goed beeld te krijgen van cultuur en gedrag, zal de auditcommissie die rapportages graag willen zien. Als het bestuur het onderwerp niet uit eigen beweging agendeert, kan de auditcommissie dat doen. Wanneer een cultuurveranderingsproces wordt ingezet, kan de auditcommissie de voortgang daarvan monitoren. De raad van commissarissen kan het bestuur vervolgens vragen stellen over de uitkomsten van de meting, de monitoring en de maatregelen die het bestuur vervolgens heeft ondernomen voor eventuele bijsturing. Overigens zijn cultuur en gedrag nooit volledig meetbaar en maakbaar. De voorzitter en de leden van de auditcommissie doen er dan ook verstandig aan zich ook **zél**f een beeld te vormen van cultuur en gedrag, mede op basis van eigen informatievergaring en observatie.

Vergaar proactief informatie
De auditcommissie gaat niet alleen af op de informatie die het bestuur uit eigen beweging verstrekt, maar heeft ook een eigen 'verlanglijstje'.

Welke interne en externe informatie geeft zicht op cultuur en gedrag?

De auditcommissie kan een beter beeld krijgen van cultuur en gedrag door proactief te vragen naar relevante informatie en daar zelf ook actief naar op zoek te gaan:

- uitkomsten van klanttevredenheidsonderzoeken;
- net promotor scores (NPS);
- meldingen bij de klachtenlijn of -commissie;
- uitkomsten van medewerkerstevredenheidsonderzoeken;
- bevindingen bij de gedragscode en het aantal meldingen van klokkenluiders;
- gegevens over medewerkersbetrokkenheid, ziekteverzuim en personeelsverloop;
- berichtgeving in het personeelsblad en op intranet;
- uitkomsten van 360-gradenfeedback;
- het proces en de uitkomsten van bestuursevaluaties;
- uitkomsten van een cultuurevaluatie: welke verschillen zijn er tussen de gewenste en de werkelijke cultuur?
- de uitkomst van stakeholderdialogen (om zicht te krijgen op de verwachtingen van stakeholders en de vraag in hoeverre de organisatie daaraan tegemoetkomt);
- berichtgeving in de media en op sociale media.

Zie ook hoofdstuk 9: Communicatie

Daarnaast kan de auditcommissie ook **zél**f actief op zoek gaan naar onafhankelijke informatie om zicht te krijgen op cultuur en gedrag. De informatie van het bestuur kan immers gekleurd of onvolledig zijn. Bovendien is het een meerwaarde voor het bestuur wanneer de toezichthouders informatie van buiten naar binnen en van beneden naar boven halen.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

- 1. Toezicht op de **purpose** en de kernwaarden
- 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
- 3. **Meten en monitoren van cultuur en gedrag**
- 4. Toetsen van de gedragscode
- 5. Voorkomen misstanden en onregelmatigheden
- 6. Verantwoording afleggen over cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Vraag om toetsing door Internal Audit

De auditcommissie kan ook een beroep doen op Internal Audit om beter zicht te krijgen op cultuur en gedrag. Deze fungeert als het geweten van de organisatie en een spiegel voor het management. Zo kan (het hoofd) Internal Audit het normenkader toetsen, een analyse maken van de risicocultuur en een thematisch onderzoek doen naar de cultuur(verandering). Dat kan ook waardevolle informatie opleveren voor de auditcommissie. Deze kan Internal Audit ook zélf vragen om cultuur en gedrag op te nemen in het jaarlijkse werkplan, bijvoorbeeld het uitvoeren van een analyse van de verschillen tussen de gewenste en de werkelijke cultuur, of de monitoring van een cultuurveranderingsproces.

Meten en monitoren cultuur

Een effectieve auditcommissie betreft Internal Audit nauw bij het meten en monitoren van cultuur. Daarbij passen vragen als: komt de werkelijke cultuur overeen met de gewenste cultuur? Ondersteunen de structuren en systemen het gewenste gedrag? Zijn de genomen beslissingen in lijn met de kernwaarden? Bovendien kan de auditcommissie het hoofd van de afdeling Internal Audit in een **private session** (die naar goed gebruik minstens een keer per jaar wordt gehouden) ook vragen naar de persoonlijke beleving van cultuur en gedrag en de eigen observaties en de zorgen bij hem of haar toetsen. Internal Audit komt immers overal in de organisatie en praat met iedereen.

Luister naar de ondernemingsraad

Ook de ondernemingsraad kan fungeren als een belangrijke interne informatiebron voor de raad van commissarissen en de auditcommissie op het gebied van cultuur en gedrag. De ondernemingsraad (OR) weet immers wat er in de organisatie speelt, wat er leeft bij de achterban en of er sprake is van zorgwekkende signalen, die wijzen op risicovol gedrag of integriteitsproblemen. Het door de auditcommissie kennisnemen van de uitkomsten van het gesprek van (een delegatie van) de raad van commissarissen met de OR kan dus bijdragen aan een beter beeld van cultuur en gedrag in de organisatie. Ook de Code verlangt dat er in het overleg tussen het bestuur, de raad van commissarissen en het medezeggenschapsorgaan gesproken wordt over cultuur en gedrag.

Vraag externe accountant om indrukken

De externe accountant vormt eveneens een belangrijke informatiebron. De accountant komt voor de controlewerkzaamheden in alle lagen van de organisatie en hoort en ziet veel. De auditcommissie kan tijdens een **private session** met de accountant vragen naar diens indruk van cultuur en gedrag van de organisatie en de eigen observaties toetsen. Dat kan waardevolle inzichten opleveren. In specifieke sectoren (zoals de financiële sector, de zorg, het onderwijs en woningcorporaties) kan ook een gesprek met de externe toezichthouder belangrijke informatie bieden: welk beeld heeft de toezichthouder van de cultuur – ook vergeleken met de rest van de sector – en welke zorgen leven er?

Praten, luisteren en observeren

De voorzitter en de leden van de auditcommissie kunnen zich een beeld vormen van cultuur en gedrag door:

- regelmatig bezoek aan de organisatie(onderdelen);
- bijwonen van formele interne bijeenkomsten (bijvoorbeeld een managersdag of vlootschouw);
- bezoek van informele interne bijeenkomsten, zoals nieuwjaarsborrels, afscheidsrecepties en feestelijke bijeenkomsten;
- meeluisteren bij calls van het management met aandeelhouders en analisten;
- aanwezig zijn bij aandeelhoudersvergadering en klantendagen;
- bijwonen van stakeholderdialogen.

Zelf zicht krijgen op cultuur en gedrag

Naast het proactief vergaren van informatie en gesprekken met bronnen als Internal Audit, de OR en de externe accountant en eventueel de externe toezichthouder, zal de auditcommissie ook zélf **the smell of the place** willen opsnuiven: wat speelt er in de organisatie, welke sfeer heerst er, hoe werken mensen samen en hoe gaan ze met elkaar en de stakeholders om? De voorzitter en de leden van de auditcommissie kunnen hun beeld van cultuur en gedrag en de risico's daarvan complementeren en verdiepen door het regelmatig bezoeken van (onderdelen van) de organisatie, het bijwonen van interne en externe bijeenkomsten, het voeren van gesprekken met medewerkers in de financiële kolom en in de rest van de organisatie en het observeren van (non-verbaal) gedrag. Daarnaast verdient het aanbeveling regelmatig het tweede echelon uit te nodigen bij de auditcommissievergadering ten

aanzien van specifieke onderwerpen. Vertoont het management voorbeeldgedrag? Hoe zijn de omgangsvormen, hoe is de onderlinge dynamiek? Hoe praten medewerkers met en over elkaar en de stakeholders? Is er sprake van respect en vertrouwen, of juist van een afrekencultuur en minachting? Zijn de rituelen, symbolen en (verborgen) boodschappen in lijn met de kernwaarden?



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

1. Toezicht op de **purpose** en de kernwaarden
2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
3. **Metten en monitoren van cultuur en gedrag**
4. Toetsen van de gedragscode
5. Voorkomen misstanden en onregelmatigheden
6. Verantwoording afleggen over cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Tien vragen over cultuur en gedrag aan de externe accountant

Commissarissen kunnen ook de externe accountant betrekken bij het toezicht op cultuur en gedrag. Ze kunnen hun observaties op dat gebied delen of toetsen tijdens de vergadering van de raad van commissarissen en/of de auditcommissie, of in een private session. Welke indruk heeft de accountant van de integratie van cultuur en gedrag in de bedrijfsvoering en de consistentie en samenhang daarvan?

1. Wat is uw indruk van het beheersingsbewustzijn in deze organisatie?
2. Wat vindt u van de mate van risicobereidheid versus de risicogedrevenheid?
3. Is er voldoende balans tussen de **hard controls** en **soft controls**?
4. Is er voldoende ruimte om fouten te maken en daarvan te leren?
5. Hoe wordt er gereageerd op incidenten?
6. Geeft het belonings- en beoordelingssysteem de juiste prikkels om het gewenste gedrag te stimuleren?
7. Wordt er voldoende en op de juiste wijze gekeken naar aspecten van cultuur en gedrag, in het kader van de jaarrekeningcontrole?
8. In welke mate zijn de kernwaarden en gedragscodes verankerd in het dagelijkse doen en laten?
9. Besteden het interne-auditplan en het controleplan van de externe accountant voldoende aandacht aan cultuur en gedrag?
10. Hoe presteren wij op deze terreinen ten opzichte van andere organisaties?



4. Toetsen van de gedragscode

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de **purpose** en de kernwaarden
 - 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
 - 3. Meten en monitoren van cultuur en gedrag
 - 4. **Toetsen van de gedragscode**
 - 5. Voorkomen misstanden en onregelmatigheden
 - 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Het bestuur stelt volgens de Code een gedragscode op, ziet toe op de werking en naleving daarvan en deelt de bevindingen en observaties daarover met de raad van commissarissen. In het toezicht door de raad van commissarissen op de gedragscode kan de auditcommissie een ondersteunende en adviserende rol spelen, voortvloeiend uit de verantwoordelijkheid voor interne controle en risicobeheersing. De gedragscode en het proces voor het bewaken van de integriteit daaromheen mogen geen doel op zich zijn, maar vormen instrumenten om integriteitsproblemen te helpen voorkomen. Het toezicht daarop mag zich niet beperken tot afvinken (is er wel of niet een gedragscode?), maar moet gericht zijn op inhoud, implementatie en monitoring: worden de juiste zaken benoemd, worden de normen en waarden in de Code doorleefd en worden deze nageleefd in de praktijk?

Vragen over de inhoud, de implementatie en de monitoring van de gedragscode
Vragen die de auditcommissie over de gedragscode en de werking en naleving daarvan kan stellen:

- Inhoud**
- Voldoet de gedragscode inhoudelijk aan alle vereisten om als een volwaardig instrument voor **soft control** te fungeren?
 - Is de gedragscode toegankelijk, leesbaar en begrijpelijk voor zowel de medewerkers als de buitenwereld?
 - Wordt de gedragscode regelmatig bijgesteld om als leidraad te fungeren voor nieuwe en actuele

- dilemma's en ethische vraagstukken?
- Voor multinationals: hoe verhoudt de gedragscode zich tot andere culturen en lokale gemeenschappen? Bevat de Code landenspecifieke richtsnoeren in de nationale taal?

- Implementatie**
- Hoe zorgt de organisatie ervoor dat alle medewerkers in de organisatie de gedragscode kennen? Is deze onderdeel van het introductie- en onboardingprogramma?
 - Committeren medewerkers zich aan de gedragscode (al of niet schriftelijk) en handelen ze ernaar in de praktijk? Leeft de gedragscode in de organisatie of is het een dode letter?

- Monitoring**
- Hoe wordt de naleving van de gedragscode gemonitord? Hebben alle medewerkers de gedragscode bevestigd? Zo nee, welke follow-upactie heeft het bestuur ondernomen? Rapporteren medewerkers proactief problemen en zorgen en zo ja: welke en hoe zijn deze aangepakt?
 - Hoeveel integriteitskwesaties zijn er geweest en hoe zijn deze aangepakt? Is er sprake van een zero-tolerancebeleid?
 - Zijn er patronen aan te wijzen in het (niet) naleven van de gedragscode die wijzen op een structureel cultuur-/integriteitsrisico in de organisatie?

Dynamisch document
Naast het aanpakken van algemene thema's als belangenverstrengeling, corruptie, fraude en organisatiespecifieke integriteitsrisico's, vormt een goede gedragscode een weerspiegeling van technologische ontwikkelingen en maatschappelijke opvattingen. De gedragscode moet dan ook regelmatig worden bijgesteld om een richtsnoer te (blijven) vormen voor het zorgvuldig en integer omgaan met actuele thema's als e-mailetiquette, privacy en seksuele intimidatie. Daarbij is het periodiek bevestigen van de naleving van de gedragscode door medewerkers een wenselijke manier om verantwoording te verankeren.

Best practice
De auditcommissie ziet toe op de monitoring van de werking en naleving van de gedragscode en kan daarvoor input of ondersteuning vragen van Internal Audit, de complianceofficer en/of bijvoorbeeld de integriteitscommissie, afhankelijk van de wijze waarop de organisatie de toetsing heeft ingericht.

Best practice
Lees gedragscodes van andere organisaties: welke thema's worden daarin op welke manier aangepakt? Put uit ervaringen bij andere toezichtposities: wat kan daarvan worden geleerd voor de beoordeling van de implementatie en de monitoring van de gedragscode?



5. Voorkomen misstanden en onregelmatigheden

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de **purpose** en de kernwaarden
 - 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
 - 3. Meten en monitoren van cultuur en gedrag
 - 4. Toetsen van de gedragscode
 - 5. **Voorkomen misstanden en onregelmatigheden**
 - 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Een gezonde cultuur kan misstanden en onregelmatigheden helpen voorkomen. Ondanks alle aandacht voor cultuur en gedrag en de monitoring daarvan, houden medewerkers zich soms echter niet aan geschreven en ongeschreven regels. Gedragscodes kunnen integriteitsschendingen niet altijd voorkomen. Het bestuur en de raad van commissarissen moeten dan ook voortdurend alert zijn op signalen van misstanden en onregelmatigheden – zoals

belangenverstrengeling, omkoping en (boekhoud) fraude – of het vermoeden daarvan. Het is van groot belang dat medewerkers deze veilig kunnen melden aan het bestuur (of aan de voorzitter van de raad van commissarissen, als het om het functioneren van een bestuurder gaat). Het bestuur stelt daarvoor een klokkenluidersregeling op, neemt signalen serieus en volgt meldingen op. De raad van commissarissen ziet daarop toe.

Bepaal de materialiteit van misstanden en onregelmatigheden

Het bestuur moet de voorzitter van de raad van commissarissen direct informeren over (vermoedens van) materiële misstanden en onregelmatigheden. Kennelijk hoeven niet alle misstanden en onregelmatigheden te worden gemeld, alleen de materiële, dat wil zeggen: de issues met de grootste impact, die het bedrijf de meeste schade kunnen toebrengen.

De auditcommissie kan de materialiteit van misstanden en onregelmatigheden anders invullen dan het bestuur en/of de externe accountant. In dat geval worden onoorbare zaken niet gemeld, waarvan de auditcommissie wel op de hoogte wil zijn voor een eigen risico-inschatting. Een effectieve auditcommissie maakt de eigen definitie van materialiteit dan ook duidelijk kenbaar naar het bestuur en de externe accountant en maakt heldere afspraken over wanneer welke issues gemeld moeten worden aan de auditcommissie.

De materialiteit van misstanden en onregelmatigheden kan bijvoorbeeld worden gebaseerd op:

- een financiële grens;
- de gevoeligheid van de kwestie, ook voor de reputatie;
- de ernst vanuit ethisch oogpunt; of:
- de betrokkenheid van senior management en managers/medewerkers in de financiële kolom.



De rol van de auditcommissie

Toetsen klokkenluidersregeling

Wat is de rol van de auditcommissie om de raad van commissarissen bij het toezicht op de klokkenluidersregeling te ondersteunen? Vanuit de verantwoordelijkheid voor compliance en de interne risicobeheersings- en controlesystemen, zal de auditcommissie het volgende willen weten, zeker als ook de integriteit van de financiële verslaggeving in het geding is:

- Is er een klokkenluidersregeling aanwezig?
- Is de regeling geschreven in de lokale taal?
- Hoe leesbaar/toegankelijk is de tekst van de klokkenluidersregeling voor de beoogde lezer? Geeft de regeling in de ogen van de auditcommissie duidelijke handvatten?
- Hoe effectief is de regeling?
- Hoe gaat het bestuur om met meldingen? Is er sprake van een zerotolerancebeleid?
- Gaat het bij meldingen om incidenten of om structurele misstanden en onregelmatigheden?
- Worden gebleken zwakke plekken in de risicosystemen versterkt?
- Wat zeggen misstanden en onregelmatigheden over cultuur en gedrag: is bijstelling noodzakelijk?
- Wat wordt er geleerd van meldingen/incidenten?

Maak de drempel voor melding zo laag mogelijk

Belangrijk is dat de organisatie de drempel voor meldingen zo laag mogelijk maakt, anonimiteit waarborgt en onderzoek/actie naar aanleiding van de melding garandeert. Wanneer er veel meldingen

van misstanden binnenkomen is dat zorgwekkend, wanneer er nooit meldingen binnenkomen is dat eveneens reden tot ongerustheid. Functioneert de klokkenluidersregeling dan wel goed? Daarnaast is het raadzaam om naast de klokkenluidersregeling andere mogelijkheden en kanalen voor het melden van misstanden en onregelmatigheden in het leven te roepen, zoals een vertrouwenspersoon, een integriteitsfunctionaris of de voorzitter van de integriteitscommissie, indien deze aanwezig is. De auditcommissie/raad van commissarissen kan deze functionarissen periodiek uitnodigen in de vergadering om verslag te doen.

Alert zijn op waarschuwingssignalen en triggers voor ongewenst gedrag

Het hebben van een effectieve klokkenluidersregeling en andere meldingsmogelijkheden is belangrijk voor het tijdig ontdekken van misstanden en onregelmatigheden. De auditcommissie zal echter zelf ook alert zijn op verborgen signalen van integriteitsrisico's, gedragsproblemen binnen de cultuur of een zwak ontwikkeld normbesef. Een open oog voor waarschuwingssignalen en perverse prikkels voor ongewenst gedrag kan risicovol gedrag en integriteitsproblemen vroegtijdig signaleren en aanpakken en daarmee erger voorkomen. Zie hiervoor ook hoofdstuk 4: Control & Compliance.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

1. Toezicht op de **purpose** en de kernwaarden

2. Toetsen van de gewenste cultuur versus de werkelijke cultuur

3. Meten en monitoren van cultuur en gedrag

4. Toetsen van de gedragscode

5. **Voorkomen misstanden en onregelmatigheden**

6. Verantwoording afleggen over cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

Verborgen signalen

De raad van commissarissen (en de auditcommissie) moet alert zijn op al of niet verborgen signalen van een ongezonde cultuur.

Voorbeelden:

- het taalgebruik van het bestuur. De zin: ‘We hebben waarden voor onze medewerkers geformuleerd’ kan duiden op een niet-authentieke en mogelijk ongezonde cultuur;
- bestuurders die liever zelf aan het woord zijn, dan vragen naar de mening van de medewerkers of de stakeholders;
- bestuurders die negatief spreken over een andere bestuurder wanneer de desbetreffende bestuurder niet aanwezig is;
- inconsistentie tussen hetgeen gezegd wordt en het eigen handelen, bijvoorbeeld benoemen dat duurzaamheid hoog op de agenda staat, maar er zelf niet naar handelen door bijvoorbeeld een zeer onzuinige auto te rijden;
- het belonen van prestaties die behaald zijn met gedrag dat niet strookt met de beleden normen en waarden.



Building a supportive environment for ethics matters

Awareness of four building blocks of an ethics programme – a key part of creating a ‘supportive environment for ethics’ – has grown from 2021 to 2024, including **written standards of business conduct** (71%, up from 67%), **confidential speak up mechanisms** (61%, up from 57%), **ethical standards training** (60%, up from 52%) and **access to advice or a helpline** (53%, up from 46%)



Most concerning is that, **of those reporting misconduct, 20% reported being aware of sexual harassment in the workplace** and **13% were aware of bribery or corruption**



Encouragingly, there is also a three-year upward trend in **willingness to speak up** (64%, up from 57%) and **satisfaction with speak up outcomes** (71%, up from 62%). Overall, **84% of employees reported that they felt that honesty is practised** in their organisations



While it is reassuring that most employees chose to speak up about misconduct, **those who did not speak up feared that no corrective action would be taken** (34%) or that **they might jeopardise their job** (34%), with no change in these two figures since 2021



However, whilst **most employees (71%) believe their organisations are taking ethics seriously**, stubbornly high levels of misconduct remain, **with 25% reporting that they had been aware of misconduct or illegal activity at work in the last year**, up from 18% in 2021.



Bron: Ethics at Work. 2024 international survey of employees, Institute of Business Ethics.

Best practice

Integriteitsproblemen zijn tot op zekere hoogte te voorzien. Voorkom de ‘voorspelbare verrassing’ door een scherp oog voor ontwikkelingen in de buitenwereld. Grijp incidenten bij andere organisaties, onderzoeksrapporten van externe toezichthouders of discussie in de (sociale) media over maatschappelijke issues aan voor een dialoog met het bestuur: Is ook in onze organisatie sprake van ongewenst gedrag ten aanzien van deze thema’s?

6. Verantwoording afleggen over cultuur en gedrag

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
 - 1. Toezicht op de **purpose** en de kernwaarden
 - 2. Toetsen van de gewenste cultuur versus de werkelijke cultuur
 - 3. Meten en monitoren van cultuur en gedrag
 - 4. Toetsen van de gedragscode
 - 5. Voorkomen misstanden en onregelmatigheden
- 6. Verantwoording afleggen over cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Het bestuur wordt volgens de Code geacht in het bestuursverslag een toelichting te geven op de waarden en de wijze waarop deze worden ingebed in de organisatie en de werking en naleving van de gedragscode. Er wordt niets gezegd over het afleggen van verantwoording door de commissarissen over de manier waarop zij toezicht hebben gehouden op cultuur en gedrag en wat de belangrijkste kwesties daarin waren. Communiceren over cultuur en gedrag in het verslag van de commissarissen hóeft dus niet, maar komt wel tegemoet aan de behoefte van stakeholders aan transparantie over dit thema.

Communiceren over soft controls

De auditcommissie kan in haar deel van het verslag van de raad van commissarissen bij het afleggen van verantwoording over het risicobeheer niet alleen ingaan op de **hard controls**, maar ook op de **soft controls**:

- Hoe heeft de auditcommissie aandacht besteed aan de meting en monitoring van de (verandering) van cultuur en gedrag?
- Hoe zijn de specifieke risico's op dit gebied verkleind, bijvoorbeeld in de beloningsstructuur?
- Was er sprake van misstanden en onregelmatigheden en hoe zijn die aangepakt?

Transparantie over missers en incidenten

Organisaties vinden het vaak moeilijk om open te zijn over zaken die (bijna) misgingen of tegenvielen, incidenten en integriteitsschendingen. Ze zijn bang voor een verslechtering van hun concurrentiepositie, negatieve reacties van aandeelhouders en andere stakeholders en een nadelig effect op hun reputatie. Het is echter een teken van kracht wanneer een organisatie uit eigen beweging ook de dingen durft te benoemen die niet goed of minder goed gingen en aangeeft hoe daarmee is omgegaan. Bovendien komt de organisatie daarmee tegemoet aan de maatschappelijke roep om transparantie en het afleggen van verantwoording. Die openheid kan juist een positief effect hebben op de reputatie, achterdocht wegnemen ("Ze houden niets achter") en bijdragen aan het vertrouwen in de organisatie.

Dat geldt ook voor het afleggen van verantwoording over cultuur en gedrag: de auditcommissie ziet erop toe dat het bestuur in het jaarverslag rapporteert over cultuur en gedrag en daarbij voldoende transparantie betracht. Zo kan het bestuur bijvoorbeeld aangeven met welke hindernissen of vertraging het cultuurveranderingsproces werd geconfronteerd, welke risico's bij de monitoring van cultuur en gedrag naar voren zijn gekomen en wat de leerpunten waren en tot welke verbetermaatregelen dat heeft geleid. Zie ook hoofdstuk 9: Communicatie.

Verslag over Business Ethics

Arcadis beschrijft de governance rondom Business Ethics. Hierin komen de Arcadis Business Principles (AGBP) langs, de inrichting van de Global Compliance Committee en de rapportagelijnen naar de Raad van Commissarissen. Het beleid en de procedures worden besproken, zoals integrity lines en ook hoe de monitoring en verantwoordelijkheid is geregeld. Verder is een paragraaf over Dealing with Dilemma's opgenomen dat gaat over de inschattingen en dilemma's bij specifieke situaties. Arcadis moedigt haar werknemers aan om, als ze deze tegenkomen, dilemma's over integriteit bespreekbaar te maken zodat er sprake is van een veilige speak-up cultuur. Er is een jaarlijkse training voor business ethics waarin voorbeelden worden gedeeld en lessons learned. Arcadis beschrijft in dit hoofdstuk ook dat er bijvoorbeeld 208 meldingen zijn geweest over mogelijk niet volgen van AGBP en dat de meeste meldingen betrekking hadden op ongewenst gedrag op de werkvloer. Tevens zijn 11 mensen ontslagen zijn op basis van het niet volgen van AGBP.

Bron: Arcadis Annual integrated report 2024, Making Sustainable Choices, Pagina 185- 187





Checks & Balances

Samenwerken met Internal Audit en de externe accountant

06

6. Checks & Balances

Samenwerken met Internal Audit en de externe accountant

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De auditcommissie kan bij het uitoefenen van haar taken en verantwoordelijkheden gebruikmaken van twee belangrijke ‘bondgenoten’: Internal Audit en de externe accountant. Met hun organisatiebrede contacten, onafhankelijke positie en objectieve blik vormen ze een extra set ogen en oren van de auditcommissie.

In dit hoofdstuk komen de volgende onderwerpen aan de orde:
A. de relatie met Internal Audit; en
B. de relatie met de externe accountant.



A. De relatie met Internal Audit

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
 - A. De relatie met Internal Audit
 1. Rolinvulling en mandaat
 2. Mensen, middelen en competenties
 3. Scope en missie
 4. Rapportage en opvolging
 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 1. Selecteren en voordragen voor benoeming
 2. Beoordelen en bewaken van de onafhankelijkheid
 3. Formuleren van de opdracht (scope, materialiteit en budget)
 4. Communiceren met de externe accountant
 5. Evalueren van het functioneren
7. Corporate Reporting
8. Crisis
9. Communicatie

In dit deel komen de volgende onderwerpen aan de orde:

A. De relatie met Internal Audit

1. Rolinvulling en mandaat
2. Mensen, middelen en competenties
3. Scope en missie
4. Opvolging aanbevelingen en relatie
5. Evaluatie en beoordeling



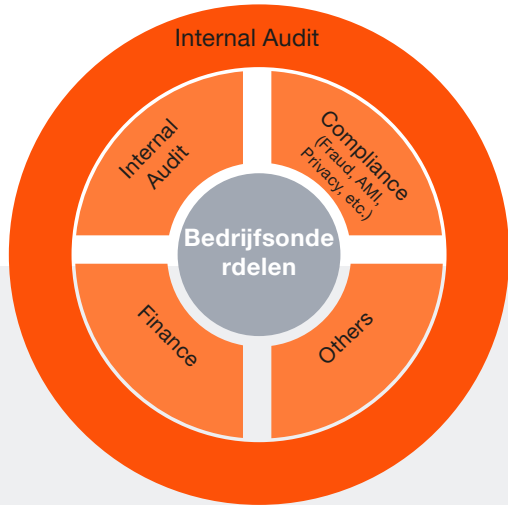
- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Natuurlijke partner, extra informatiebron en intern geweten

De auditcommissie moet goed zicht hebben op de effectiviteit van de risicobeheersings- en controlesystemen. De auditcommissie bereidt immers de besluitvorming voor van de raad van commissarissen, die toezicht houdt op de interne beheersing en controle. Daarbij gaat het niet alleen om financiële, maar ook om niet-financiële risico's, niet alleen om hard controls, zoals functiescheiding en procedures, maar ook om soft controls, zoals cultuur en gedrag. Bovendien brengen de snelle veranderingen in de externe omgeving voortdurend nieuwe risico's met zich mee, zoals de disruptieve gevolgen van nieuwe technologie.

‘Third line of defence’

Internal Audit is een natuurlijke partner voor de auditcommissie bij de beoordeling van het dynamische risicoprofiel en de monitoring van de strategie-uitvoering en het primaire proces. De primaire taak van Internal Audit is de beoordeling van de opzet en de werking van de interne risicobeheersings- en controlesystemen. De herziening van de Code heeft de afgelopen jaren geleid tot een verbreding van de scope en een verzwaring van de rol van Internal Audit. De discipline heeft zich ontwikkeld tot een **third line of defence**, naast de beheersing in het primaire proces en de governance-, risk- en compliancefuncties in de tweede lijn. Overigens spreekt The Institute of Internal Auditors (IIA) sinds 2020 liever over het **three lines model**. In dat model blijft Internal Audit de onafhankelijke derde lijn, met een coördinerende rol in het geheel.



Mogelijke onderwerpen voor onderzoeken door Internal Audit:

- aanwijzingen voor mogelijke fraude;
- naleving van wet- en regelgeving;
- klokkenluidersregeling;
- uitgaven bestuur;
- voortgang van projecten.

Internal Audit kan ook workshops geven aan het bestuur over de risico's die de basis vormen van het jaarlijkse auditprogramma.

Het IIA wil met de naamswijziging echter benadrukken dat de functies niet alleen zijn bedoeld om de waarde van de organisatie te beschermen maar ook om deze te vergroten.

Moreel kompas

Internal Audit licht de organisatieprocessen door en komt daardoor in diverse geledingen en op veel niveaus van de organisatie. Internal Audit opereert onafhankelijk en functioneert bovendien als moreel kompas. Daarmee is Internal Audit een belangrijke bron voor het vergaren van onafhankelijke en objectieve informatie voor de auditcommissie, naast de informatie die door het bestuur wordt verstrekt. De auditcommissie kan Internal Audit dan ook inzetten voor het verkrijgen van een breed overzicht van en een diep inzicht in de organisatie. Het hoofd Internal Audit is het directe aanspreekpunt voor de auditcommissie.

Prominente rol in governancecode

De auditcommissie kan dus een beroep doen op Internal Audit om zicht te krijgen op de beheersing van het gehele risicopalet van de organisatie, zowel toekomstig, strategisch, operationeel als tactisch en zowel hard als zacht. Dat vraagt om een nauwe relatie tussen de auditcommissie en Internal Audit. De Code stelt dat de raad van commissarissen toezicht houdt op de interne auditfunctie en regelmatig contact heeft met degene die de functie vervult. De auditcommissie speelt daarbij een centrale rol en fungeert als vooruitgeschoven post:

- De auditcommissie adviseert het bestuur bij benoeming, beoordeling en ontslag van Internal Audit.
- Internal Audit betreft de auditcommissie bij het opstellen van het werkplan.

- De auditcommissie bereidt goedkeuring van het werkplan van Internal Audit door de raad van commissarissen voor.
- Internal Audit heeft direct toegang tot de auditcommissie.
- Er wordt vastgelegd op welke manier Internal Audit de auditcommissie informeert.
- Internal Audit rapporteert de kern van de onderzoeksresultaten aan de auditcommissie.

Binnen deze kaders kunnen de auditcommissie en Internal Audit hun eigen invulling geven aan de relatie en de rapportage.

Vijf bouwstenen voor een effectieve relatie met Internal Audit

De auditcommissie helpt het hoofd of het team Internal Audit denken en acteren op het gewenste strategische niveau om waarde toe te voegen aan het governanceproces. De auditcommissie kan Internal Audit als discipline in zijn kracht zetten en expliciet aangeven wat de verwachtingen zijn ten aanzien van de invulling van de rol, de gewenste vaardigheden en competenties van het hoofd en het team Internal Audit, de scope van de werkzaamheden en de manier van rapporteren. De auditcommissie kan die verwachtingen duidelijk maken door goed gebruik te maken van de vijf bouwstenen voor een effectieve relatie met Internal Audit:

1. de vaststelling van het charter (reglement);
2. de opstelling van het werkplan;
3. de bespreking van de periodieke rapportages;
4. het onderhouden van tussentijdse contacten;
5. de jaarlijkse beoordeling van Internal Audit.

1. Rolinvulling en mandaat

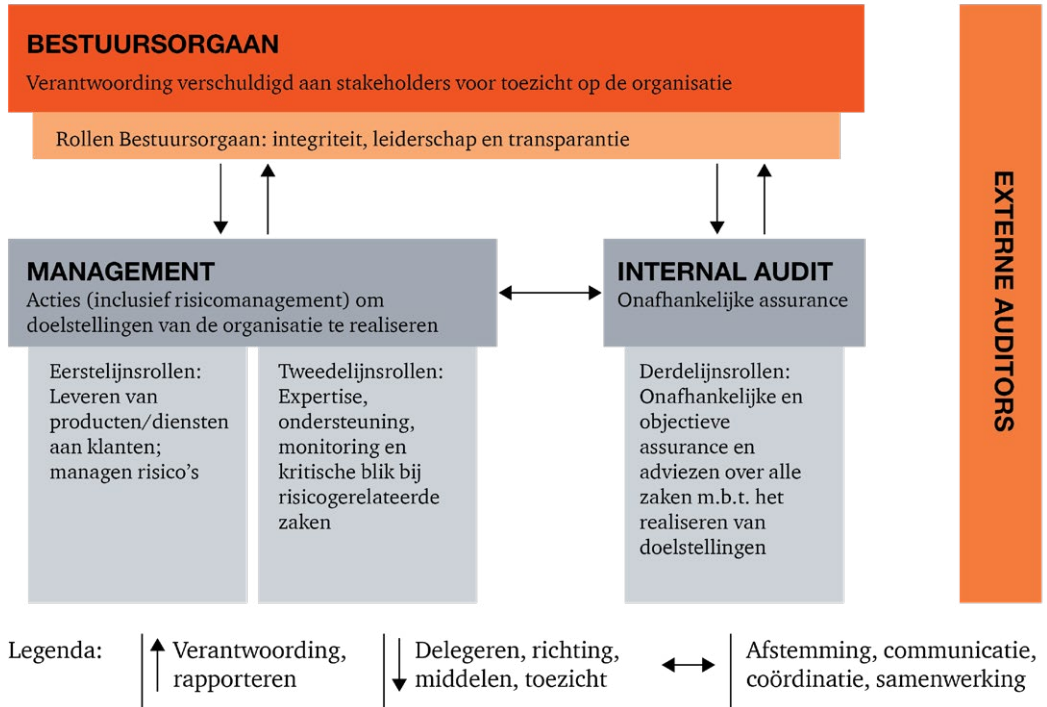
- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Bij de prominente plaats die Internal Audit toebedeeld heeft gekregen in governance, past een proactieve rol. Effectieve interne audit gaat verder dan alleen de controle van de interne risico- en beheersingssystemen en voorziet de auditcommissie ook van oorzakenanalyses van zwakheden of problemen in de interne beheersing en governance en suggesties voor structurele verbeteringen. Internal Audit kan ook proactief zijn, bijvoorbeeld door te participeren in belangrijke projecten om deze aan de voorkant te helpen vormgeven: met de juiste **checks & balances**, SMART geformuleerde doelen en monitoring.

Check het charter van Internal Audit

- Bij het opstellen en (jaarlijks) evalueren van het charter van Internal Audit kan de auditcommissie zich de volgende vragen stellen:
- Blijkt uit het charter duidelijk wat de scope is van de werkzaamheden van Internal Audit en is dit overeengekomen met de auditcommissie?
 - Heeft Internal Audit voldoende middelen en bevoegdheden om aan haar verplichtingen te voldoen?
 - Worden in het charter de rapportagelijnen voor de afdeling Internal Audit benoemd? En zo ja, zijn deze voldoende om aan de behoeftes van de leden van de auditcommissie te voldoen?
 - Eist het charter dat het hoofd Internal Audit regelmatig bijeenkomt met de auditcommissie zonder het bestuur, of faciliteert het directe toegang tot de voorzitter van de auditcommissie?
 - Welke samenhang is er tussen Internal Audit en andere borgingsmaatregelen?
 - Wanneer is het charter voor het laatst geactualiseerd en vernieuwd? Is het charter nog actueel voor wat betreft de bedrijfsactiviteiten en voor wat betreft de veranderende wet- en regelgeving en naleving?
 - Worden in het charter de standaarden benoemd die Internal Audit moet hanteren? Bijvoorbeeld de Global Internal Audit Standards van het IIA?

In de rol van **trusted advisor** denkt Internal Audit ook mee over het creëren van waarde in de toekomst, door het in kaart brengen van kansen en risico's voor het businessmodel en de strategie en zo te fungeren als sparringpartner van het bestuur en de auditcommissie. Welke gevolgen heeft bijvoorbeeld nieuwe technologie: opent deze nieuwe markten, of dreigt juist disruptie? De auditcommissie kan ook een beroep doen op Internal Audit voor monitoring van de executie van de (nieuwe) strategie.



Vastlegging in het charter

Om de rol van **trusted advisor** goed en met autoriteit te kunnen vervullen, heeft Internal Audit een stevig mandaat nodig: hij of zij moet zich gesteund voelen door het bestuur en de auditcommissie, binnen de organisatie in die rol geaccepteerd worden en toegang hebben tot alle relevante informatie. Rolinvulling, autoriteit en mandaat worden vastgelegd in een charter, net als taken en verantwoordelijkheden, de scope van de werkzaamheden en rapportagelijnen.

Best practice

Agendeer standaard een **private session** met Internal Audit, voorafgaand of na de vergadering van de auditcommissie.



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie



Alle belanghebbenden bedienen

In theorie is het eenvoudig: Internal Audit heeft een onafhankelijke positie binnen de organisatie met een hiërarchische lijn naar het bestuur (en een stippellijn naar de auditcommissie). In de praktijk wordt Internal Audit door meerdere belanghebbenden benaderd, wat kan leiden tot lastige keuzes. Zo moet Internal Audit ook aansluiting houden met het lijnmanagement, met de tweedelijns functies en leggen toezichthoudende instanties (vooral in de financiële sector) steeds meer opdrachten (indirect) bij Internal Audit neer. Het is voor Internal Audit in de praktijk soms lastig om al deze belanghebbenden goed te bedienen.



Rapportagelijnen

Internal Audit heeft zowel een relatie met de auditcommissie als met het bestuur. Daarom zijn heldere rapportagelijnen en het vastleggen daarvan van groot belang. Internal Audit rapporteert aan de voorzitter van het bestuur (de ceo). Ook heeft Internal Audit direct toegang tot de auditcommissie en de externe accountant. Internal Audit rapporteert de onderzoeksresultaten aan het bestuur, de kernpunten van de onderzoeksresultaten aan

de auditcommissie en informeert de externe accountant.

In de praktijk is er dan ook frequent contact tussen Internal Audit en de auditcommissie. De Code spreekt eveneens over ‘regelmatig contact’ van de raad van commissarissen met degene die de interne-auditfunctie vervult, een taak die veelal door de auditcommissie wordt ingevuld. In het charter wordt vastgelegd hoe de auditcommissie door Internal Audit wordt geïnformeerd en hoe vaak en op welke manier de auditcommissie en Internal Audit met elkaar communiceren.

‘Private sessions’

Internal Audit is standaard aanwezig bij elke vergadering van de auditcommissie. Daarbuiten is het niet ongebruikelijk dat er ook informeel contact is tussen de auditcommissie en het hoofd Internal Audit, zonder aanwezigheid van het bestuur. Gemiddeld genomen vinden deze **private sessions** tussen de auditcommissie en Internal Audit een tot twee keer per jaar plaats, hoewel sommige voorzitters van de auditcommissie voorafgaand aan elke vergadering apart overleggen met Internal Audit.

Die **private sessions** hebben een grote toegevoegde waarde: de auditcommissie kan dan immers vrijelijk vragen naar de observaties van Internal Audit. Wat ziet of hoort hij of zij in de organisatie, wat speelt er? De auditcommissie kan ook de eigen observaties delen en toetsen: herkent Internal Audit die? Zijn er signalen en waarschuwingstekens waarop de auditcommissie alert moet zijn?

2. Mensen, middelen en competenties

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
 - A. De relatie met Internal Audit
 1. Rolinvulling en mandaat
 2. Mensen, middelen en competenties
 3. Scope en missie
 4. Rapportage en opvolging
 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 1. Selecteren en voordragen voor benoeming
 2. Beoordelen en bewaken van de onafhankelijkheid
 3. Formuleren van de opdracht (scope, materialiteit en budget)
 4. Communiceren met de externe accountant
 5. Evalueren van het functioneren Bijlagen
7. Corporate Reporting
8. Crisis
9. Communicatie

Internal Audit moet beschikken over de mensen en middelen om de taken en verantwoordelijkheden op het gewenste strategische niveau te kunnen vervullen en de rol van **trusted advisor** te kunnen spelen. Ook is het belangrijk dat het hoofd Internal Audit of het team over de juiste vaardigheden en competenties beschikt: inhoudelijk vakkundig, autonoom denkend, onafhankelijk opererend en met rechte rug. Een goede manier om de kwaliteit van Internal Audit te borgen (en intern draagvlak te creëren) is om de functie, het team of de afdeling onderdeel te maken van het leadership development van potentiële bestuurders van de organisatie. Het transformeren van de interne- auditfunctie of -afdeling tot een ‘doorgangshuis’ of springplank voor talent – waarbij high potentials na drie tot vijf jaar doorstromen naar (andere) managementfuncties – kan leiden tot een hoogwaardiger bezetting en een regelmatige verversing. Dit leidt ook tot een betere relatie tussen Internal Audit en de business.

Diversiteit en flexibiliteit

Het heeft de voorkeur dat de samenstelling van het interne-auditteam divers en dynamisch is: de organisatie, de externe omgeving en de bijbehorende risico’s zijn immers ook voortdurend in beweging. Er zijn diverse manieren om de interne-auditfunctie daadwerkelijk in te vullen, sommige organisaties hebben hiervoor een functionaris of afdeling in eigen huis, andere besteden alle werkzaamheden uit. Ook een hybride benadering is mogelijk: externe ondersteuning wordt ingehuurd als er onvoldoende capaciteit aanwezig is om het jaarplan te realiseren of wanneer specifieke expertise intern niet voorhanden is, bijvoorbeeld voor de

audit van (nieuwe) regelgeving (zoals IFRS, EU AI Act, CSRD of GDPR), een IT-systeem of een cultuurverandering.

Als werkzaamheden van Internal Audit worden uitbesteed is het van belang dat de auditcommissie vaststelt dat de ingehuurde functionarissen gekwalificeerd en objectief zijn. Ook dan gelden dezelfde hoge verwachtingen ten aanzien van de kwaliteit van de interne audit.



3. Scope en missie

- 1. Commissie
 - 2. Continuïteit
 - 3. Corporate impact
 - 4. Control & Compliance
 - 5. Cultuur en gedrag
 - 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
 - Bijlagen
- 7. Corporate Reporting
 - 8. Crisis
 - 9. Communicatie

De Code verwacht dat Internal Audit een brede scope hanteert bij de controle en advisering en zich richt op het gehele risicoprofiel: strategisch, operationeel en tactisch, financieel en niet- financieel, **hard controls** en **soft controls**.

Werkplan en opdrachten voor onderzoek

De auditcommissie is betrokken bij het jaarplan van Internal Audit en kan de gewenste scope aangeven, plus een specifiek verlanglijstje neerleggen, zoals:

- onderwerpen die aansluiten bij de strategie van de onderneming en de voornaamste bedrijfsrisico's;
- onderwerpen gerelateerd aan disruptieve trends en toekomstige risico's en kansen;
- beheersing van bijzondere projecten, projectmanagement, nieuwe contracten;
- voldoende ruimte in het werkplan van Internal Audit om ad hoc onderzoeken op te pakken.

Daarnaast kan de auditcommissie specifieke opdrachten voor gericht onderzoek aan Internal Audit verstrekken en ook daarmee sturen op de scope en het gewenste niveau. Daarnaast is het ook aan te bevelen om halverwege het jaar samen met Internal Audit te bekijken of het jaarplan bijstelling behoeft.

Visie op rolontwikkeling en toekomstige toegevoegde waarde

Naast het jaarplan, kan de auditcommissie ook samen met Internal Audit verkennen hoe Internal Audit toegevoegde waarde kan leveren en welke toekomstvisie voor het hoofd Internal Audit en het team van toepassing is.

Daarbij horen vragen als:

- Welke rol zou Internal Audit in de governance moeten spelen?
- Hoe gaat Internal Audit daarbij om met alle stakeholders en hun verschillende belangen en verwachtingen: auditcommissie/raad van commissarissen, raad van bestuur, managers, de externe accountant en eventueel de externe toezichthouder?
- Welke rol gaat Internal Audit op termijn spelen om toegevoegde waarde te blijven bieden en is er een plan om de rol of afdeling in die richting te ontwikkelen?
- Wat betekenen ontwikkelingen als GenAI, digitalisering en robotisering voor Internal Audit? Veel handmatige controles worden geautomatiseerd: wat betekent dat voor de controlehouding, de vormgeving van de audits en het signaleren van nieuwe en andersoortige risico's?



De digitale transformatie van de interne audit

Beoordeel wat de visie is van Internal Audit op de nieuwste technologieën

- Maakt de organisatie al gebruik van opkomende technologieën, zoals blockchain, kunstmatige intelligentie of robotisering? Zijn er plannen om dit te gaan doen?
- Heeft de interne-auditafdeling de juiste competenties om risico's op deze gebieden in te kunnen schatten en te kunnen aanpakken in interne audits als het aankomt op zulke technologieën?
- Maakt de interne-auditfunctie gebruik van samenwerking, gegevensextractie, analytics, en visualisatietools?
- Zit er in het strategische plan van Internal Audit ook een ontwikkelplan voor technologische vaardigheden en tools?

Breng technologie en talent samen in één strategie

- Laat de doelstellingen van de organisatie leidend zijn in het toewijzen van investeringen in technologie en talent.
- Investeer nu slim, om in de toekomst de vruchten te plukken.
- Beoordeel welke digitale vaardigheden beschikbaar zijn voor Internal Audit.
- Zorg voor de ontwikkeling en inkoop van de technologische vaardigheden die nodig zijn voor de toekomst.

Probeer altijd innovatief en revolutionair te zijn

- Probeer te bedenken hoe dingen anders kunnen, in plaats van kleine verbeteringen.
- Zoek manieren om de technologieën en talenten van anderen te delen of te gebruiken om grote stappen te zetten.
- En onthoud dat het probleem van vandaag morgen niet meer bestaat; werk samen met de innovatieagenda van de organisatie om te zorgen dat Internal Audit op dit front niet achter gaat lopen.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
 - A. De relatie met Internal Audit
 1. Rolinvulling en mandaat
 2. Mensen, middelen en competenties
 3. Scope en missie
 4. Rapportage en opvolging
 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 1. Selecteren en voordragen voor benoeming
 2. Beoordelen en bewaken van de onafhankelijkheid
 3. Formuleren van de opdracht (scope, materialiteit en budget)
 4. Communiceren met de externe accountant
 5. Evalueren van het functioneren Bijlagen
7. Corporate Reporting
8. Crisis
9. Communicatie



Voorbeelden van vragen die de auditcommissie aan Internal Audit kan stellen:

- Hoe functioneren de risico- en beheersingssystemen over de volle breedte van de organisatie (ook in buitenlandse vestigingen die zich op grote afstand van het hoofdkantoor bevinden)?
- Waar in de organisatie zou zich een frauderisico kunnen voordoen en zijn er voldoende maatregelen genomen om mogelijke fraude tegen te gaan?
- Wat speelt er op de verschillende organisatieniveaus en welke cultuur- en gedragsrisico's brengt dat met zich (soft controls)?
- Hoe verloopt het cultuurveranderingsprogramma?
- In hoeverre ondersteunen de beoordelings- en beloningssystemen de strategie, de gewenste cultuur en de langetermijnwaardcreatie waarop beide zijn gericht?
- Wat is de status van de follow-upacties ten aanzien van de door de externe accountant gerapporteerde aandachtspunten?
- Welke ontwikkelingen ziet Internal Audit op het gebied van governance, risico's en naleving in de organisatie (afgezet tegen externe ontwikkelingen)?
- Hoe verlopen cruciale operationele processen en belangrijke projecten (qua kwaliteit, budget, planning en bemensing)?
- Welke voortgang wordt er gemaakt in het duurzaamheidsbeleid?
En hoe ontwikkelen we ons op het gebied van **responsible tax**?
Hoe verhoudt dat zich tot het reputatierisico?
- Welke gevolgen heeft nieuwe technologie voor het primaire proces en voor risico's op het gebied van cybersecurity?
- Hoe verloopt de uitvoering van de (nieuwe) strategie en is de interne controle daaraan aangepast?
- Welke disruptieve trends en toekomstige risico's (**emerging risks**) vragen om innovatie van het businessmodel of bijstelling van de strategie?

4. Rapportage en opvolging

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

In de rapportage van de bevindingen besteedt Internal Audit volgens de Code in elk geval aandacht aan:

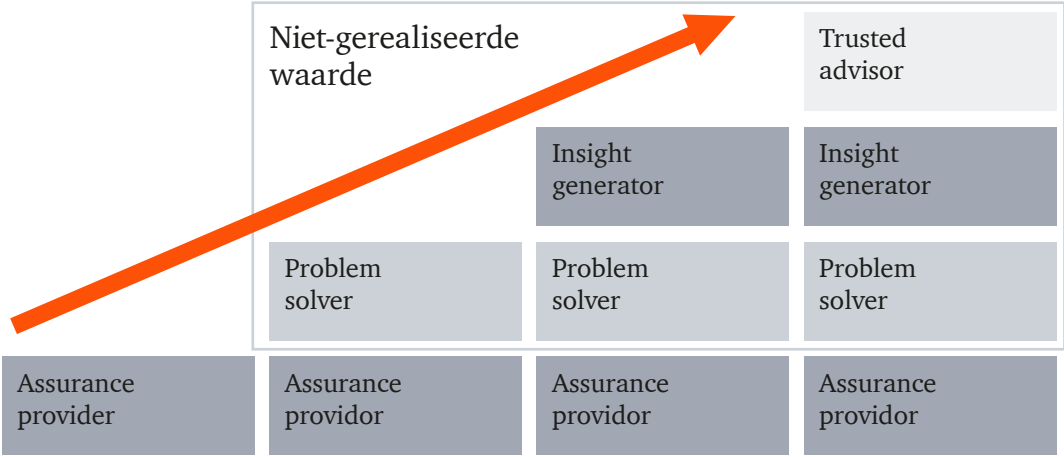
- i. gebreken in de effectiviteit van de interne risicobeheersings- en controlesystemen;
- ii. bevindingen en observaties die van wezenlijke invloed zijn op het risicoprofiel; en
- iii. tekortkomingen in de opvolging van aanbevelingen van Internal Audit.

Voor een toelichting op i) en ii) zie hoofdstuk 4: Control & Compliance.

Daarbij geeft Internal Audit zekerheid aan de auditcommissie dat de systemen goed functioneren en het bestuur ondersteunen bij het realiseren van de strategie. Internal Audit kan echter aan waarde winnen als de functie doorgroeit naar die van **trusted advisor** (zie figuur).

Hierbij kan gedacht worden aan:

- **assuranceprovider** – niet alleen over uitzonderingen en observaties rapporteren maar ook expliciet een uitspraak durven doen over de mate van **in control** zijn van de organisatie over onder meer de financiële verslaggeving, operationele processen en naleving van wet- en regelgeving;
- **probleemoplosser** – een gedegen oorzakenanalyse maken van problemen en aanbevelingen doen om fouten te voorkomen (**second loop learning**) en de beheersing verder te verbeteren;
- **insight generator** – voortbouwend op de oorzakenanalyse, de auditcommissie inzicht geven in structurele ontwikkelingen in de risico's en de interne risicobeheersings- en controlesystemen en adviezen geven over het beheersen van projecten,



Uit de praktijk
Het interne-auditteam van een grote bank presenteerde de onderzoeksresultaten als experiment niet in een closingmeeting maar in een gallery walk: op de ramen hingen grote sheets die de audit in beeld brachten. Het bestuur kon er langs wandelen, in plaats van een rapport te moeten doorworstelen. De verantwoordelijke chieft audit executive: ‘Prachtig vond men het. Een rapport met aanbevelingen over de schutting gooien, kan echt niet meer. Het rapport is slechts een middel.’ Het gaat om de dialoog tussen de raad van commissarissen, de auditcommissie, het bestuur en Internal Audit over wat wordt gerapporteerd.

Opvolging rapportage-items van Internal Audit
De rapportage van Internal Audit aan de auditcommissie bevat meestal een overzicht van de belangrijkste bevindingen:

- aantal bestaande issues
- aantal nieuwe issues
- aantal opgeloste issues
- aantal openstaande issues
- ouderdomsanalyse

Bijvoorbeeld: van de tien issues staan er nog negen issues open, die twee maanden geleden al opgelost hadden moeten zijn.

- Vraag als auditcommissie om het overzicht als dat geen deel uitmaakt van de rapportage van Internal Audit
- Bekijk het staatje voor de vergadering van de auditcommissie en vraag het bestuur: Hoe kan het dat deze issues nog openstaan?

Het rapport van Internal Audit voor de auditcommissie bevat naast het staatje met bevindingen vaak ook een pagina met observaties (afgestemd met het bestuur): deze observaties vormen interessante input voor vragen aan of discussie met het bestuur. Het is gebruikelijk dat Internal Audit ook rapporteert over de status van de follow-up van het bestuur op de door de externe accountant gerapporteerde bevindingen en aanbevelingen.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

A. De relatie met Internal Audit

1. Rolinvulling en mandaat

2. Mensen, middelen en competenties

3. Scope en missie

4. Rapportage en opvolging

5. Evaluatie en beoordeling

B. De relatie met de externe accountant

1. Selecteren en voordragen voor benoeming

2. Beoordelen en bewaken van de onafhankelijkheid

3. Formuleren van de opdracht (scope, materialiteit en budget)

4. Communiceren met de externe accountant

5. Evalueren van het functioneren

Bijlagen

7. Corporate Reporting

8. Crisis

9. Communicatie

het optimaliseren van risicoraamwerken of het behoud van functionarissen op sleutelposities;

- **trusted advisor** – voldoende expertise en autoriteit bezitten om mee te denken op het gebied van risicobeheersing en interne controle en over de uitvoering van de strategie.

■ De rol van de auditcommissie

Toezicht op de actiebereidheid van het bestuur

De auditcommissie houdt toezicht op de opvolging van de opmerkingen en aanbevelingen voor verbetering van Internal Audit. De auditcommissie kan bij het bestuur aandringen op het voortvarend oppakken van voorgestelde acties en suggesties en de opvolging daarvan zorgvuldig monitoren.

Toezicht op de relatie van het bestuur met Internal Audit

De auditcommissie ziet ook toe op de relatie van Internal Audit met het bestuur: krijgt hij of zij de medewerking en informatie om de taken in alle vrijheid te kunnen uitoefenen en staan het bestuur en het management open voor de bevindingen, ook als die als pijnlijk worden ervaren?

Hoe is de toon aan de top?	
Belangrijke vragen	Mogelijke antwoorden
Welke samenwerking ervaart u met zowel het bestuur als het operationele management?	Altijd goede samenwerking. Er zullen echter altijd verschillen van inzicht aanwezig zijn. Deze moeten worden toegelicht, zodat de auditcommissie kan beoordelen wat de visie van alle betrokken partijen is en hoe de samenwerking verloopt. Serieuze verschillen van inzicht moeten worden aangepakt.
Heeft u situaties meegemaakt waarbij het bestuur of het management niet bereid was om samen te werken?	Voorbeelden helpen hierbij om het issue en de onderlinge relatie inzichtelijk te krijgen.
Is er wel eens een verzoek tot informatie geweigerd?	Nee. Internal Audit moet altijd toegang krijgen tot welke informatie zij dan ook maar wenst in te zien. Dit moet ook benadrukt worden in het reglement. Als er zorgen zijn hierover moet de auditcommissie deze analyseren en tot een oplossing zien te komen.
Op welk gebied loopt de organisatie volgens u een risico (financieel, reputatie, operationeel, et cetera)	Een duidelijke toelichting waaruit een goed begrip blijkt van de risico's, en waaruit voldoende blijkt dat deze worden opgepakt door Internal Audit of op andere wijze geborgd worden (indien van toepassing).
Is het benoemen van deze aandachtsgebieden onderdeel van uw interne-auditplan?	De enige wijzigingen die zijn toegestaan aan rapporten zijn feitelijke onjuistheden. Internal Audit moet erop toezien dat alle belangrijke risico's die zij vaststelt gedurende interne controles worden gerapporteerd aan de auditcommissie.
Is er op on gepaste wijze druk op u uitgeoefend om bevindingen vanuit uw werkzaamheden aan te passen of op andere wijze te prioriteren?	Als er zorgen zijn dat er op on gepaste wijze druk wordt uitgeoefend, dan moet de auditcommissie met het hoofd van Internal Audit bespreken door wie deze druk wordt uitgeoefend en hoe hij of zij denkt dit op te gaan lossen.



5. Evaluatie en beoordeling

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren Bijlagen
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De auditcommissie wordt (door het bestuur) betrokken bij de jaarlijkse beoordeling van de wijze waarop Internal Audit de taken uitvoert.

Scorecard en dashboard

De auditcommissie kan voor de beoordeling gebruikmaken van een zelfevaluatie van Internal Audit aan de hand van een scorecard of dashboard, als deze zijn opgenomen in het auditrapport. De zelfevaluatie betreft bijvoorbeeld het aantal audits, het al of niet behalen van targets, de tevredenheid van de interne klant, het aantal aanbevelingen en de snelheid waarmee deze worden opgepakt.

Soft skills

Het gaat bij de beoordeling van Internal Audit echter niet alleen om harde prestatiecriteria, maar ook om zachte. Internal Audit moet niet alleen onderzoek goed uitvoeren, maar de uitkomsten daarvan ook kunnen vertalen naar overkoepelende thema’s en trends en deze in de context van het bedrijf kunnen plaatsen. Bovendien is het van belang dat het hoofd Internal audit beschikt over **soft skills**. Het is gewenst dat hij of zij een goede gesprekspartner is voor de auditcommissie, de raad van commissarissen en het bestuur: over een goede boardroompresence beschikt, kan omgaan met bestuurlijke dynamiek en zich onafhankelijk opstelt, ook wanneer druk wordt uitgeoefend.

Internationale benchmark voor beoordeling Internal Audit

Het Internal Audit Ambition Model is een tool voor zelfevaluatie van het IIA. Met dit model kan (het hoofd van) Internal Audit het bestaande kwaliteitsniveau in kaart brengen en de ambities benoemen om de functie verder te professionaliseren: wat wil Internal Audit bereiken en wat is daarvoor nodig? In het ambitiemodel komen de volgende thema’s aan de orde:

- rol Internal Audit;
- beleid, processen en best practices voor professioneel en effectief opereren;
- peoplemanagement;
- prestatie management en verantwoording afleggen;
- relaties in de organisatie en cultuur;
- governancestructuren.

De resultaten van het ambitiemodel worden vergeleken met het kwaliteitsniveau van andere Internal Audit-functies in eigen land en wereldwijd. Ook voor de auditcommissie levert deze (inter)nationale benchmark waardevolle informatie op voor de beoordeling van Internal Audit.



Externe kwaliteitstoetsing (door Internal Audit)

Op basis van het Reglement Kwaliteitstoetsing van IIA Nederland moet elke interne auditfunctie met een of meer leden van het IIA zich een keer per vijf jaar extern laten toetsen aan de IIA-standaarden, door een gekwalificeerde organisatie (zoals het IIA).

Het doel hiervan is om de kwaliteit van de beroepsuitoefening door de leden te verhogen door uitspraak te doen over de mate waarin het interne stelsel van kwaliteitsbeheersing in opzet en werking voldoet aan de algemeen aanvaarde normen voor de beroepsuitoefening. Hierbij wordt ook gekeken hoe Internal Audit wordt gewaardeerd door de stakeholders en welke verbetermogelijkheden er zijn om de toegevoegde waarde van Internal Audit te verhogen.



Advies over benoeming en ontslag van het hoofd van Internal Audit

De auditcommissie kan zich over het functioneren van Internal Audit een oordeel vormen door goed te observeren tijdens de formele en informele contacten met het hoofd Internal Audit en het interne auditteam. De auditcommissie brengt overigens ook advies uit aan het bestuur over de benoeming en het ontslag van het hoofd Internal Audit. Het bestuur legt de benoeming of het ontslag vervolgens voor aan de raad van commissarissen.

Als Internal Audit in de organisatie ontbreekt

Als de interne auditdiscipline niet apart is belegd in de organisatie, dan moet de auditcommissie jaarlijks advies uitbrengen aan de raad van commissarissen of er adequate alternatieve maatregelen zijn getroffen en of er behoefte bestaat aan een interne-auditdienst. De raad van commissarissen moet de conclusies van het oordeel daarover en de eventuele aanbevelingen en alternatieve maatregelen opnemen in het eigen verslag in het jaarverslag.

In het advies aan de raad van commissarissen moet de auditcommissie in ieder geval aandacht besteden aan de volgende onderwerpen:

- Op welke wijze ontvangen de raad van commissarissen en de auditcommissie onafhankelijke informatie over de interne governance, zodat er niet volledig gesteund wordt op de informatievoorziening vanuit het bestuur?
- Alternatieven ten aanzien van de invulling van de **third line of defence**, hierbij kan gedacht worden aan:

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

- het bestuur dat vanuit zijn eigen expertise een aanvullende kritische toetsende rol vervult binnen het systeem van interne governance;
- het lijnmanagement (eerste lijn) dat vooral binnen een projectmatige organisatiestructuur zelfstandig verantwoordelijk is voor de invulling van de interne governance, daarbij vaak ondersteund én kritisch bevraagd door sterke ‘hoofdkantoorfuncties’;
- de controlfunctie (tweede lijn) die vooral door de toegenomen professionaliteit van de businesscontrollers ingezet wordt als een extra onafhankelijke en kritische blik richting de vaak complexe business;
- de externe accountant (vierde lijn), vooral als een efficiënter en effectiever alternatief voor de interne-auditfunctie als het gaat om het uitvoeren van financiële of IT-controlewerkzaamheden in het kader van de jaarrekeningcontrole;
- Kunnen we op basis van de aard van de business, het risicoprofiel en de strategie van de organisatie, uitleggen richting de buitenwereld dat we, in tegenstelling tot de best practice, geen interne-auditfunctie hebben ingericht?

Checklist voor de beoordeling van het hoofd Internal Audit

- Visie
- vertaalt zijn of haar visie in een strategisch interne auditplan;
 - investeert in competenties waarmee de visie gerealiseerd kan worden;
 - geeft effectief leiding aan het interne-auditteam;

- Talent
- focus op mentorschap en talentontwikkeling;
 - zet talenten in om waarde te creëren en maakt waar nodig gebruik van externe expertise;

- Positie
- heeft draagvlak bij de belangrijkste stakeholders;
 - maakt effectief gebruik van zijn of haar onafhankelijke rol;
 - ondersteunt het voorbeeldgedrag van het bestuur;
 - neemt verantwoordelijkheid in het bouwen van een positie ten opzichte van het bestuur en de auditcommissie;
 - beschikt over grondige kennis en begrip van de business;



- Communicatie
- is zelfbewust, straalt rust en vertrouwen uit, is authentiek en toont integer gedrag;
 - communiceert op een evenwichtige, krachtige en resultaatgerichte manier;
 - dwingt respect af bij de stakeholders, ook buiten de context van een specifieke controle;
 - weet duidelijk aan te geven wat de waarde is van de interne audit;

- Businessalignment
- zorgt voor een goede aansluiting van Internal Audit op de strategie, de kernwaarden en de samenhangende risico's;
 - ontwikkelt solide relaties gebaseerd op wederzijds respect en vertrouwen;
 - bouwt en onderhoudt partnerships tussen de verschillende **lines of defence**;
 - gebruikt actief het interne netwerk om de betrokkenheid bij risico's en maatregelen te verstevigen.

Voorbeeld van een interne-auditcharter:



B. De relatie met de externe accountant

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
 - A. De relatie met Internal Audit
 1. Rolinvulling en mandaat
 2. Mensen, middelen en competenties
 3. Scope en missie
 4. Rapportage en opvolging
 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 1. Selecteren en voordragen voor benoeming
 2. Beoordelen en bewaken van de onafhankelijkheid
 3. Formuleren van de opdracht (scope, materialiteit en budget)
 4. Communiceren met de externe accountant
 5. Evalueren van het functioneren
7. Corporate Reporting
8. Crisis
9. Communicatie



In dit deel komen de volgende onderwerpen aan de orde:

B. De relatie met de externe accountant

1. Selecteren en voordragen voor benoeming
2. Beoordelen en bewaken onafhankelijkheid
3. Formuleren van de opdracht (scope, materialiteit en budget)
4. Communiceren met de externe accountant
5. Evalueren van het functioneren

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Cruciaal samenspel
Een kerntaak van de auditcommissie is de beoordeling van de integriteit en kwaliteit van de financiële en niet-financiële verslaggeving, ter voorbereiding van het toezicht en de besluitvorming van de raad van commissarissen op dit gebied. Die taak lijkt uitdagender dan ooit, in een tijdperk van toenemende regelgeving, de roep om transparantie, hoge maatschappelijke verwachtingen en de noodzaak tot vertrouwensherstel. Een goed samenspel van de auditcommissie met de externe accountant is cruciaal voor integere verslaggeving en een effectief controleproces.

Opdrachtrelatie versus informatie uitwisselen
De relatie tussen de auditcommissie en de externe accountant heeft een tweezijdig karakter. Aan de ene kant vervult de auditcommissie (als vooruitgeschoven post van de raad van commissarissen) de rol van opdrachtgever. De auditcommissie:

- is verantwoordelijk voor de selectie van de externe accountant;
- adviseert de raad van commissarissen over de voordracht tot benoeming en ontslag van de externe accountant;
- doet een voorstel voor de controleopdracht;
- bespreekt het controleplan, de tussentijdse bevindingen en de uitkomsten van de controle;
- beoordeelt het functioneren van de externe accountant; en
- beoordeelt en monitort de onafhankelijkheid van de externe accountant.

Aan de andere kant is de externe accountant een belangrijke informatiebron voor de auditcommissie. De externe accountant doorkruist bij de controlewerkzaamheden immers de gehele organisatie, praat met veel mensen in de organisatie en overziet de inzet van het management, de medewerkers en de middelen. Dat kan leiden tot waardevolle en objectieve observaties voor het toezicht op de organisatie. Op zijn beurt kan de externe accountant het beeld van de verslaglegging en de gang van zaken in de organisatie complementeren en toetsen aan de hand van de informatie die de auditcommissie van het bestuur en door eigen inspanning heeft verkregen.

Samenwerking tussen de auditcommissie en de externe accountant
De relatie tussen de auditcommissie en de externe accountant gaat dus verder dan die tussen opdrachtgever en opdrachtnemer rond het controleren van de cijfers. De samenwerking is gebaseerd op een aantal opmerkelijke overeenkomsten: de auditcommissie en de externe accountant houden beide toezicht op basis van een maatschappelijk mandaat, opereren daarbij vanuit de positie van onafhankelijke buitenstaander en hebben een gemeenschappelijk doel: een gedegen en deugdelijke verantwoording van de organisatie aan de stakeholders. Ze kunnen elkaar helpen en versterken. Een goede samenwerking tussen de auditcommissie en de externe accountant is gebaat bij intensieve interactie, openheid, oprechtheid en wederzijds vertrouwen.

Effectief samenwerken: vijf verantwoordelijkheden
Wet- en regelgeving schetsen de basis voor de samenwerking door het benoemen van de taken en verantwoordelijkheden van de auditcommissie voor een effectieve relatie met de externe accountant (zie het overzicht in bijlage 6A).

Aanloopfase - voor de opdracht

- beoordeling van de prestaties van de externe accountant in het afgelopen jaar: het controleteam, de dienstverlening en het honorarium;
- bespreking van het controlevoorstel – benadering dienstverlening, voorwaarden en honorarium;
- beoordeling van de onafhankelijkheid van de accountant en de ervaring van het controleteam;
- overweging van de opdrachtbevestiging;
- opstelling benoemingsvoorstel voor de raad van commissarissen.

Afrondingen (na einde jaar)

- beoordeling van de gecontroleerde jaarrekening;
- bespreking van de belangrijkste controlebevindingen – belangrijkste waarderingsgrondslagen / oordelen / kwaliteit van de financiële verslaglegging;
- bespreking van eventuele meningsverschillen met het management;
- aparte bespreking met de externe accountant;
- beoordeling van de prestaties.

Het is echter aan de auditcommissie zelf om op dit fundament een sterke relatie te bouwen met de externe accountant om tot een krachtig samenspel te komen. Daarin pakt de auditcommissie proactief haar rol in alle fasen van het externe controleproces, van de selectie tot en met de evaluatie.

Inzicht krijgen in het controleplan

- bespreking en goedkeuring van het controleplan voor het lopende jaar;
- uiteenzetting van de verwachtingen van de accountant, namelijk dienstverlening, tijdspad en rapporteringsvereisten;
- beoordeling van de manier waarop de belangrijkste risicogebieden worden behandeld gedurende de controle.

Op de hoogte blijven gedurende de controle

- op de hoogte zijn van de problemen die men tegenkwam tijdens de uitvoering van de controle;
- beperkingen met betrekking tot de toegang tot informatie/het management;
- op de hoogte zijn van tekortkomingen in de interne controle/fraude/onwettige daden;
- op de hoogte zijn van kwesties die van invloed zijn op de onafhankelijkheid van de accountant.

1. Selectie en voordracht benoeming

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De auditcommissie is verantwoordelijk voor de procedure voor de selectie van de externe accountant en de voordracht voor (her) benoeming aan de algemene vergadering van aandeelhouders. Die voordracht vindt plaats door de raad van commissarissen, op advies van de auditcommissie.

Verplichte roulatie
Nederland kent een verplichte roulatie van de externe accountant voor organisaties van openbaar belang (OOB): deze organisaties moeten minimaal één keer per tien jaar wisselen van accountantskantoor. Daarna geldt een afkoelingsperiode van vier jaar voor een eventuele herbenoeming van hetzelfde kantoor.

Daarnaast zijn er regels met betrekking tot de (maximale) lengte (zeven jaar) van de periode van betrokkenheid van senior leden van het assuranceteam bij dienstverlening aan de organisatie. Voor OOB's geldt echter dat de eindverantwoordelijke accountant en de eventuele andere key assurancepartners maximaal vijf, respectievelijk zeven jaar betrokken mogen zijn bij een assuranceopdracht bij de OOB; daarna geldt een afkoelingsperiode van drie jaar.

Best practice
Bespreek met de externe accountant periodiek het opvolgingsplan voor het assuranceteam om de continuïteit te waarborgen.

De rol van de auditcommissie
Aanbeveling en motivatie
De auditcommissie bereidt de selectie van de externe accountant voor en geeft advies aan de raad van commissarissen over de voordracht van benoeming van de externe accountant. De auditcommissie betreft hierin de observaties van het bestuur. Als uitkomst van de selectieperiode moet de auditcommissie één partij (voor OOB's twee partijen) voordragen aan de aandeelhouders en daarbij een voorkeur uitspreken: wie is op dit moment de beste accountant voor de organisatie? De aanbeveling van de auditcommissie bevat ten minste twee keuzemogelijkheden voor de controleopdracht en een gemotiveerde keuze voor één daarvan. De motivatie daarbij moet ingaan op de inhoudelijke argumenten voor de keuze, zoals de gehanteerde methodologie, de match met en kwaliteit van het team, individuele expertise van de teamleden en gebruik van technologie. Het verdient aanbeveling om de keuze en de overwegingen daarbij schriftelijk vast te leggen.

Meewegen van de prijs
Een onderdeel van elke offerte is de prijs. Het uitgangspunt is een faire prijs voor een hoogwaardige controle met toegevoegde waarde. Gezien het belang van het kwalitatieve deel van de offerte, kan ervoor gekozen worden om de prijsinformatie apart te laten aanleveren. De prijs wordt dan pas onthuld als de selectiecommissie haar inhoudelijke voorkeur heeft uitgesproken voor een van de inschrijvers. Denk ook goed na over de mate waarin, naast

de kwalitatieve aspecten, de prijs meeweegt in de uiteindelijke keuze. De prijs zou niet van dominante invloed mogen zijn op de keuze voor de accountant. Primair moet de accountantscontrole bijdragen aan de verantwoordelijkheid van de auditcommissie. Betrek bij deze evaluatie ook de reikwijdte (scope) van de aanbidding. Merk hierbij op dat het bestuur mogelijk eerder zal kiezen voor een zo laag mogelijke prijs om de impact op de winst-en-verliesrekening zo laag mogelijk te houden. De auditcommissie houdt zich dus regelmatig bezig met de selectie- en (her) benoemingsprocedure. Organisaties in de semipublieke sector hebben bij de selectie van de externe accountant vaak te maken met een Europese aanbestedingsprocedure. Zie bijlage 6B voor een overzicht van de belangrijkste componenten van en tips voor het selectieproces.

Pak de regie
Een goede samenwerking met de externe accountant begint met de selectie. De auditcommissie moet vanaf het begin bij het selectieproces betrokken zijn, zich opstellen als opdrachtgever en de regie nemen. Wat zijn best practices hiervoor?

- Focus op de persoonlijke relatie. Een klik tussen de voorzitter en de leden van de auditcommissie met het controleteam zorgt voor een effectieve controlerelatie. Bij wederzijdse bereidheid en vertrouwen worden gevoelige kwesties eerder openlijk met

Best practice
Vraag als auditcommissie bij de selectie van auditteams: 'Hoe ga je om met onderbuikgevoelens die je niet vanuit feiten kunt staven?' of 'Wat is het grootste professionele dilemma geweest dat u in uw rol van accountant het afgelopen jaar hebt ervaren?'

elkaar besproken en zorgen gedeeld.

- Maak tijdens het offerteverzoek (ook) kennis met het controleteam waarmee de auditcommissie contact zal hebben.
- Stel vragen die zicht bieden op de meerwaarde van de externe accountant voor de organisatie en de auditcommissie (zie bijlage 6C).
- Kijk of het professioneel en persoonlijk klikt met de lead auditpartner en de mensen die het eigenlijke werk gaan doen.
- Observeer: hoe is de samenwerking en de cultuur in het controleteam?

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

A. De relatie met Internal Audit

1. Rolinvulling en mandaat
2. Mensen, middelen en competenties
3. Scope en missie
4. Rapportage en opvolging
5. Evaluatie en beoordeling

B. De relatie met de externe accountant

1. Selecteren en voordragen voor benoeming
2. Beoordelen en bewaken van de onafhankelijkheid
3. Formuleren van de opdracht (scope, materialiteit en budget)
4. Communiceren met de externe accountant
5. Evalueren van het functioneren

7. Corporate Reporting

8. Crisis

9. Communicatie

Mogelijke criteria voor de selectie van de externe accountant	sector kennis in de organisatie en in het team.	• transitieplan.
Het team • samenstelling van het team (vaardigheden en ervaring van de individuele teamleden en van het team als geheel); • commitment (tijd) van de belangrijkste (kern) teamleden; • persoonlijke klik en communicatie; • beschikbaarheid specialistische kennis; • beschikbaarheid, kwaliteit en ervaring van (buitenlandse) controleteams; • beleid voor continuïteit in het team; • omgang met vaktechnische beslissingen; • enthousiasme en eagerness voor de opdracht; • curricula vitae van de teamleden.	Aanpak en scope • inrichting controleaanpak, inclusief risicoanalyse, scope en materialiteit; • technologie in de controleaanpak; • onderscheidend vermogen en meerwaarde van/in de controleaanpak; • de coördinatie van de controlewerkzaamheden; • ervaring en mandaat van het groepsteam bij het aansturen van andere controleteams en specialisten; • stimuleren zelfcontrolerend vermogen van de organisatie; • samenwerking met Internal Audit of andere relevante afdeling(en); • invulling van de natuurlijke adviesfunctie.	De organisatie • referenties in de sector; • potentiële conflicten; • kwaliteitsbewakingssysteem; • cultuuraspecten: matchen de normen en waarden van de organisatie met die van de inschrijvers. Honorarium • prijs-kwaliteitverhouding; • gedetailleerde breakdown van de controle-uren en het honorarium naar bijvoorbeeld businessunit en functieniveaus; • (rand)voorwaarden.
Sector kennis • ervaring en expertise in de sector (inclusief ervaring met relevante toezichthouders); • visie op (recente) ontwikkelingen in de sector en de impact op de organisatie; • het inspelen op (interne en externe) ontwikkelingen; • borging en kennisdeling van	Communicatie • rapportage aan het management en de aandeelhouders; • invulling van de communicatie gedurende het jaar. Transitie • ervaring met transitie(s) bij vergelijkbare organisaties;	



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

A. De relatie met Internal Audit

1. Rolinvulling en mandaat
2. Mensen, middelen en competenties
3. Scope en missie
4. Rapportage en opvolging
5. Evaluatie en beoordeling

B. De relatie met de externe accountant

1. Selecteren en voordragen voor benoeming
2. Beoordelen en bewaken van de onafhankelijkheid
3. Formuleren van de opdracht (scope, materialiteit en budget)
4. Communiceren met de externe accountant
5. Evalueren van het functioneren
Bijlagen

7. Corporate Reporting

8. Crisis

9. Communicatie

Expliciteer en toets de visie op de samenwerking

- Maak verwachtingen van de samenwerking en specifieke wensen meteen kenbaar in het selectiedocument: accountantsfirma's kunnen daar dan al rekening mee houden bij de samenstelling van het controleteam;
- Gebruik de presentatie van controleteams om de invulling van de rol en de visie op de samenwerking te toetsen: komen deze overeen met de visie en verwachtingen van de auditcommissie en zijn de juiste attitude en competenties aanwezig, zoals oog voor **soft controls**?
- Kijk bij de selectie tijdig naar de bestaande adviesrelaties met externe accountants. Weeg het strategische belang daarvan af tegen de eventuele selectie als externe accountant: welke dienstverlening is belangrijker

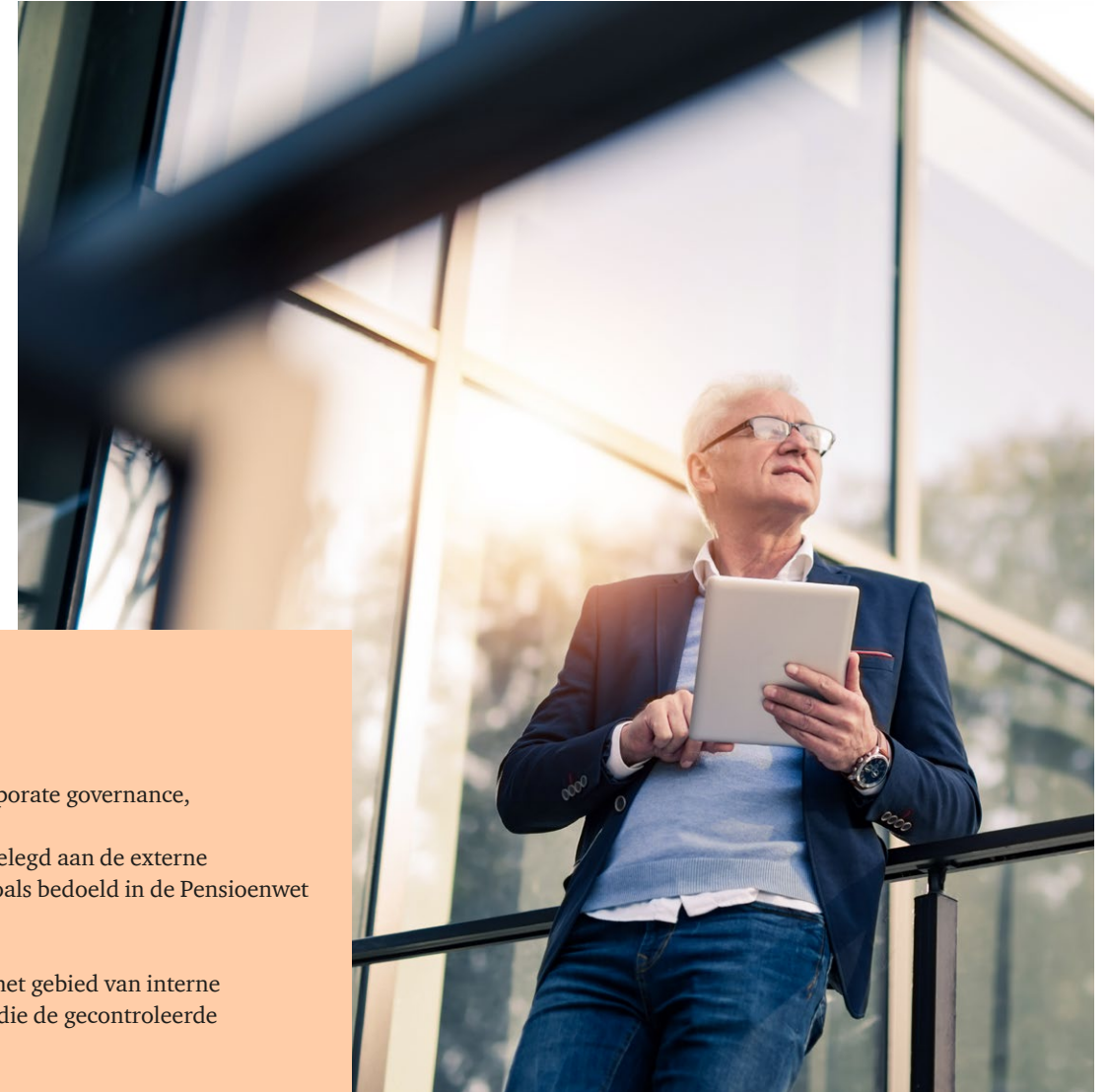
voor de organisatie? De Nederlandse onafhankelijkheidsregelgeving ten aanzien van de wettelijke controle van OOB's sluit immers het verlenen van andere diensten dan wettelijk gedefinieerde controlediensten door de externe accountant uit. Zie ook bijlage 6D.

- Betrek de observaties van het bestuur en Internal Audit bij de voordracht tot her(benoeming).
- Maak de selectiecriteria en de belangrijkste conclusies van de raad van commissarissen over de voordracht en de uitkomsten van het selectieproces openbaar aan de algemene vergadering van aandeelhouders (zodat aandeelhouders op basis van die informatie een gefundeerde beslissing kunnen nemen om de voorgedragen externe accountant al of niet te benoemen).

De definitie 'controlediensten'

Controlediensten omvatten in Nederland uitsluitend:

- de (wettelijke) controle van de jaarrekening of de geconsolideerde jaarrekening;
- de controle of de beoordeling van (en tussen de) financiële overzichten;
- het verstrekken van assurance met betrekking tot andere aspecten van de jaarverslaggeving, zoals corporate governance, risicomanagement of maatschappelijk verantwoord ondernemen;
- elke andere wettelijke taak die verband houdt met controlewerkzaamheden die door wetgeving is opgelegd aan de externe accountant of de accountantsorganisatie (zoals de waarmerking van staten voor de toezichthouder, zoals bedoeld in de Pensioenwet en de Wet op het financieel toezicht);
- het verstrekken van assurance en feitenonderzoek voor externe gebruikers (zoals comfort letters);
- het verstrekken van assurance en feitenonderzoek voor de raad van commissarissen (bijvoorbeeld op het gebied van interne beheersing, fusies en overnames en fraude). De diensten moeten betrekking hebben op de informatie die de gecontroleerde organisatie verstrekt heeft.



2. Beoordeling en bewaking van de onafhankelijkheid

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Het is de taak van de auditcommissie om de onafhankelijkheid van de externe accountant te beoordelen en te monitoren tijdens de selectieprocedure en gedurende de gehele periode dat het accountantskantoor als externe accountant van de organisatie functioneert.

Analyse van bedreiging van de onafhankelijkheid

De externe accountant moet voorafgaand aan het aanvaarden of continueren van een wettelijke controleopdracht een analyse maken van eventuele bedreigingen op het gebied van de persoonlijke onafhankelijkheid van het assuranceteam:

- als gevolg van bestaande en eventueel voorgenomen niet-controledienstverlening door de externe accountant aan de organisatie;
- ten gevolge van eventueel bestaande andere zakelijke relaties (zoals samenwerkingsverbanden en inkooprelaties; de externe accountant moet vaststellen of adequate maatregelen zijn getroffen om deze bedreigingen weg te nemen of te mitigeren. De externe accountant moet de uitkomsten van deze analyse documenteren en bespreken met de auditcommissie.

Specifieke regelgeving voor OOB's en EU PIE's

Nieuw in de EU-regels is dat er sprake is van een afkoelingsperiode van een jaar met betrekking tot de door de te benoemen externe accountant geleverde diensten op het gebied van: **designing and implementing internal**

control or risk management procedures related to the preparation and/or control of financial information or financial information technology systems. De externe accountant kan niet worden benoemd als deze dergelijke diensten heeft verleend in het jaar voorafgaand aan het eerste te controleren boekjaar. Ten aanzien van assurance bij het duurzaamheidsverslag op grond van de CSRD gelden vergelijkbare onafhankelijkheidseisen.

Met betrekking tot OOB's en EU PIE's zijn de verantwoordelijkheden van de auditcommissie (en van de externe accountant) op het gebied van de onafhankelijkheid bij de invoering van de EU PIE-regelgeving meer expliciet gemaakt en uitgebreid. Belangrijke aspecten zijn:

- De auditcommissie moet alle wettelijk toegestane en door de onderneming gewenste niet-controledienstverlening vooraf goedkeuren.
- Een Nederlandse externe accountant mag geen andere diensten dan (de wettelijk vastgelegde) controlediensten verlenen aan de Nederlandse OOB, de moedermaatschappij(en) van de OOB, dan wel aan in de EU gevestigde dochtermaatschappijen van de OOB (meer dan vijftig procent zeggenschap).
- Buitenlandse netwerkfirma's verbonden aan de externe accountant mogen aan in Nederland gevestigde groepsmaatschappijen ook alleen controlediensten verlenen.

Aan in het buitenland gevestigde groepsmaatschappijen (meer dan vijftig procent zeggenschap) mogen zij niet-controlediensten verlenen, indien en voor zover deze toegestaan zijn onder de in het land van vestiging geldende onafhankelijkheidsregels.

- De auditcommissie moet ook richtlijnen toepassen voor het inhuren van de externe accountant voor bepaalde belastingadvieswerkzaamheden (waaronder de belastingaangifte) ten behoeve van de organisatie) en waarderingsdiensten ten behoeve van groepsmaatschappijen in EU-lidstaten waar dat onder voorwaarden is toegestaan.
- Voor OOB's geldt bovendien een honorariumplafond van zeventig procent van het gemiddelde honorarium voor de wettelijke controle als bovengrens voor de door de externe accountant te leveren andere diensten. Zie voor een uitgebreide toelichting bijlage 6D.

Best practices voor toetsing van de onafhankelijkheid van de externe accountant

- Bepaal (of pas) het eigen beleid (aan) ten aanzien van het door de externe accountant en zijn of haar netwerk verlenen van (niet-controle)dienstverlening aan de organisatie en groepsmaatschappijen, houd hierbij ook rekening met de onafhankelijkheidsregelgeving in het land van vestiging van de diverse groepsmaatschappijen. Overweeg welke opdrachten de auditcommissie zelf wil goedkeuren en voor welke opdrachten de goedkeuring wordt gedelegeerd aan

Best practice

Expliciteer de visie op de samenwerking in het selectiedocument, bijvoorbeeld: 'We verwachten dat de externe accountant zijn beeld over de organisatie vrijelijk deelt met de auditcommissie, ook als het controleteam dat liever niet schriftelijk vastlegt.'

bijvoorbeeld het hoofd Internal Audit. Dit kan afhankelijk zijn van de aard en/of de hoogte van het honorarium van de opdracht.

- Stem het beleid met de externe accountant af (en publiceer dit op de website).
- Wees er zeker van dat de procedure van voorafgaande goedkeuring ten aanzien van niet-controlediensten door de externe accountant adequaat is en goed werkt.
- Vraag de externe accountant ten minste één keer per jaar schriftelijk om een overzicht van alle verleende niet-controlediensten en een bevestiging dat een en ander in overeenstemming is met van toepassing zijnde regelgeving en dat de onafhankelijkheid van de externe accountant gedurende het jaar niet is aangetast.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
 - A. De relatie met Internal Audit
 1. Rolinvulling en mandaat
 2. Mensen, middelen en competenties
 3. Scope en missie
 4. Rapportage en opvolging
 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 1. Selecteren en voordragen voor benoeming
 2. Beoordelen en bewaken van de onafhankelijkheid
 3. Formuleren van de opdracht (scope, materialiteit en budget)
 4. Communiceren met de externe accountant
 5. Evalueren van het functioneren
7. Corporate Reporting
8. Crisis
9. Communicatie

Belangrijke vragen voor toetsing van de onafhankelijkheid van de externe accountant

Gedurende het selectieproces

- Wat zijn de interne procedures en systemen van de (eventueel te benoemen) externe accountant op het gebied van het voldoen aan op de organisatie van toepassing zijnde onafhankelijkheidsregelgeving?
- Is de externe accountant (en de accountantsorganisatie) de afgelopen jaren door toezichthouders aangesproken op gebreken en/of overtredingen van onafhankelijkheidsregelgeving?
- Hoe weten we dat op het moment van benoeming alle (mogelijke) bedreigingen van de onafhankelijkheid van de externe accountant zijn geïdentificeerd en tijdig zijn opgelost?
- Welke diensten kunnen eventueel worden voortgezet indien de accountantsorganisatie als externe accountant wordt benoemd?



3. Formulering van de opdracht aan de externe accountant (scope, materialiteit en budget)

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

A. De relatie met Internal Audit

- 1. Rolinvulling en mandaat
- 2. Mensen, middelen en competenties
- 3. Scope en missie
- 4. Rapportage en opvolging
- 5. Evaluatie en beoordeling

B. De relatie met de externe accountant

- 1. Selecteren en voordragen voor benoeming
- 2. Beoordelen en bewaken van de onafhankelijkheid
- 3. Formulieren van de opdracht (scope, materialiteit en budget)
- 4. Communiceren met de externe accountant
- 5. Evalueren van het functioneren Bijlagen

7. Corporate Reporting

8. Crisis

9. Communicatie

De auditcommissie doet een voorstel aan de raad van commissarissen voor de opdracht voor de controle van de jaarrekening aan de externe accountant. Bij het formuleren van de opdracht moet de auditcommissie ook aandacht besteden aan de reikwijdte van het accountantsonderzoek (de scope) en de te hanteren materialiteit.

Informatie is volgens de Nederlandse richtlijnen van de Raad voor de Jaarverslaggeving en de internationale verslaggevingsstandaarden (IFRS) van materieel belang wanneer ‘het weglaten of het onjuist weergeven daarvan de economische beslissingen die gebruikers op basis van de jaarrekening nemen, zou kunnen beïnvloeden’. De materialiteit van de post of fout is niet alleen afhankelijk van de omvang, maar ook van de aard ervan.

Best practices voor de formulering van de opdracht:

- Vorm een eigen mening over de gewenste scope en materialiteit van de opdracht en draag die expliciet uit naar de externe accountant en de raad van commissarissen.
- Deel kennis van risico's en specifieke zorgpunten met de externe accountant, zodat deze de scope en de materialiteit daarop kan afstemmen.
- Hanteer bij de scope en de materialiteit van de opdracht (en het controleplan) een brede definitie, die ook ruimte biedt voor controle van informatie en issues van niet-financiële aard, zoals langetermijnwaardcreatie en cultuur, duurzaamheid en diversiteit.
- Bepaal de betrokkenheid van de externe

accountant bij de inhoud en publicatie van financiële berichten anders dan de jaarrekening, zoals halfjaarcijfers, kwartaalcijfers en persberichten. Dit kan bijvoorbeeld in de vorm van een beoordelingsopdracht of opdracht tot specifiek overeengekomen werkzaamheden.

Best practice

Wees alert op verandering in scope en materialiteit bij de wisseling van accountant en de mogelijke vragen van aandeelhouders daarover.

Bepalen en bewaken honorarium externe accountant

- Maak als auditcommissie nadrukkelijk de eigen visie op de reikwijdte en het bijbehorende budget van de externe accountant kenbaar: het bestuur heeft als gecontroleerde partij wellicht andere belangen dan de auditcommissie.
- Selecteer op kwaliteit en inhoud, niet alleen, of vooral, op prijs.
- Schep in het budget ruimte voor regelmatig informeel overleg tussen de auditcommissie en de externe accountant, bijvoorbeeld voorafgaand en na afloop van de vergadering van de auditcommissie.

Belangrijkste vragen voor de formulering van de opdracht aan de externe accountant

Voorbeeldvragen met betrekking tot de controleaanpak van de externe accountant:

- Wat zijn de doelstellingen van uw controle?
- Welke eisen worden er aan de financiële verslaggeving van de onderneming gesteld en hoe luidt de tijdsplanning om hieraan te voldoen?
- Op welke gebieden bent u van plan tijdens uw controle de nadruk te leggen? Waarom?
- In welke mate gaat u het interne beheersingssysteem van de onderneming beoordelen?
- In welk opzicht zal de jaarrekening van dit jaar worden beïnvloed door recente wijzigingen in grondslagen van financiële verslaggeving en/of eisen die door regelgevers/toezichthouders worden gesteld?
- Hoe zullen recente transacties en handelingen van de onderneming, zoals fusies en overnames, herstructureringen, wijzigingen in de ondernemingsstrategie, wijzigingen in financieringsafspraken, of andere ongebruikelijke transacties, uw controle of verklaring beïnvloeden?
- Wat is uw controleaanpak met betrekking tot de geautomatiseerde systemen en applicaties van de onderneming?
- Hoe coördineert u uw werkzaamheden met de interne auditor?
- Welke bedrijfsvestigingen zult u dit jaar bezoeken? Bezoekt u steeds andere bedrijfsvestigingen? Zo ja, hoe bepaalt u welke vestigingen u wanneer bezoekt?
- Welke dochtermaatschappijen gaat u controleren? Welke stappen onderneemt u met betrekking tot de niet-gecontroleerde dochtermaatschappijen?
- Indien hierbij andere accountantsfirma's zijn betrokken, hoe stelt u de aanvaardbaarheid van hun werkzaamheden en hun onafhankelijkheid vast?
- Wat zijn uw verantwoordelijkheden voor het ontdekken van fouten van materiële betekenis, fraude en onwettige handelingen?
- Hoe deelt u met ons de belangrijkste discussiepunten met het bestuur over uw concept-rapportage van interim-bevindingen en op basis daarvan aangebrachte wijzigingen in uw rapportage van interim-bevindingen?



4. Communicatie met de externe accountant

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De basis van de communicatie tussen auditcommissie en de externe accountant is vastgelegd in de Code. Zo legt de externe accountant het concept-controleplan aan de auditcommissie voor. Vervolgens moet de auditcommissie jaarlijks een aantal zaken met de externe accountant bespreken, zoals de reikwijdte en materialiteit van het controleplan en de belangrijkste risico's van de jaarverslaggeving die de externe accountant daarin heeft benoemd. De auditcommissie bespreekt ook jaarlijks de tussentijdse bevindingen van de

Valkuil

Voorkom dat alleen de auditcommissie met de externe accountant praat. Geef ook de overige commissarissen gelegenheid voor 'reguliere contacten' met de externe accountant om vragen te stellen, observaties te delen en hun eigen oordeel te vormen. De gehele raad van commissarissen heeft baat bij de inzichten en onafhankelijke mening van de externe accountant. De externe accountant is minimaal één keer per jaar aanwezig in de vergadering met de voltallige raad van commissarissen. Best practice is een staande uitnodiging voor commissarissen die niet in de auditcommissie zitten om de vergaderingen van de auditcommissie bij te wonen en hen toegang te geven tot alle documentatie voor de auditcommissie. Zie hoofdstuk 9: Communicatie.

externe accountant, de uitkomsten van de controlewerkzaamheden en de rapportage van de interim-bevindingen (zie hoofdstuk 7: Corporate Reporting voor de inhoudelijke bespreking daarvan en de vragen die de auditcommissie daarbij kan stellen).

Blik van binnen en van buiten

De auditcommissie kan echter veel meer waarde halen uit de relatie met de externe accountant dan alleen het bespreken van de absoluut noodzakelijke en vereiste onderwerpen. Hier komt de meerwaarde van de accountant als extra onafhankelijke informatiebron aan bod, zowel intern als extern. De externe accountant komt immers door de gehele organisatie, maar ziet ook veel andere organisaties.

Overige onderwerpen die met de externe accountant besproken kunnen worden:

- observaties ten aanzien van het gedrag en de kwaliteit van het management in het algemeen en het financeteam in het bijzonder, de toon aan de top en de cultuur in de organisatie;
- de visie van de externe accountant op (niet-)financiële informatie, bijvoorbeeld duurzaamheidsinformatie en kwartaalrapportages, en de rol van de accountant hierbij;
- de visie van de externe accountant op business- of branchebrede risico's en maatschappelijke trends, zoals reputatierisico's en de disruptieve gevolgen van technologische ontwikkelingen als digitalisering en robotisering;

Uit de praktijk

De auditcommissie van een beursgenoteerde onderneming bespreekt tijdens de eigen vergadering de plannen voor een acquisitie in het buitenland. De auditcommissie focust daarbij vooral op strategische en financiële factoren: wat is de bijdrage van de overname aan de langetermijnwaardecreatie van de organisatie en is deze financieel haalbaar? De externe accountant kijkt verder dan de auditcommissie en betreft ook de organisatorische consequenties erbij: in de praktijk ziet de externe accountant acquisities immers vaak mislukken door een gebrekkige integratie. Die ervaring weerspiegelt zich in de twee vragen die de externe accountant stelt: 'Is het management van de organisatie ervaren genoeg om de acquisitie te behappen'? En: 'Zijn in de overnamesom de kosten meegenomen voor control van de nieuwe buitenlandse vestiging vanuit het hoofdkantoor?' De auditcommissie stelt beide vragen vervolgens aan het bestuur tijdens de commissarissenvergadering, waar de acquisitie op de agenda staat. Uiteindelijk geeft de raad van commissarissen groen licht voor de overname, op voorwaarde dat er een integratiemanager wordt benoemd en dat de kosten voor extra control in het bod worden verdisconteerd.

- best practices voor het effectief functioneren van de auditcommissie, gebaseerd op de veelvuldige contacten van de externe accountant met auditcommissies van andere organisaties.

Reguliere vergaderingen

In de praktijk is de externe accountant aanwezig bij alle vergaderingen van de auditcommissie, net als de cfo en het hoofd Internal Audit, tenzij de auditcommissie dat anders beslist. Dat laatste komt nog steeds voor. Zo mag de externe accountant soms alleen dat deel van de vergadering bijwonen dat relevant is voor de jaarrekeningcontrole. Best practice is echter dat de externe accountant de gehele vergadering bijwoont en daarbij niet alleen als toehoorder fungeert, maar een actieve inbreng kan

hebben, ook al heeft het onderwerp niet direct betrekking op de controle. De voorzitter van de auditcommissie kan de accountant daartoe uitnodigen door bij elk agendapunt expliciet om diens inbreng te vragen. De externe accountant kan op basis van zijn of haar kennis, ervaring in andere organisaties en observaties in de controle een waardevolle bijdrage leveren aan de discussie.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

A. De relatie met Internal Audit

- 1. Rolinvulling en mandaat
- 2. Mensen, middelen en competenties
- 3. Scope en missie
- 4. Rapportage en opvolging
- 5. Evaluatie en beoordeling

B. De relatie met de externe accountant

- 1. Selecteren en voordragen voor benoeming
- 2. Beoordelen en bewaken van de onafhankelijkheid
- 3. Formuleren van de opdracht (scope, materialiteit en budget)
- 4. Communiceren met de externe accountant
- 5. Evalueren van het functioneren Bijlagen

7. Corporate Reporting

8. Crisis

9. Communicatie

Private sessions

Naast de reguliere vergaderingen overlegt de auditcommissie in elk geval één keer per jaar zonder aanwezigheid van het bestuur met de externe accountant: de **private session**. Die ene verplichte **private session** per jaar vormt ook hier weer het absolute minimum. De auditcommissie heeft volgens de Code om ‘zo vaak als zij dit noodzakelijk acht’ apart te overleggen met de externe accountant (dus zonder de cfo en de ceo of andere bestuursleden).

Apart overleg voor en na vergadering

Een effectieve auditcommissie maakt goed gebruik van die ruimte om apart contact te hebben met de externe accountant. Sommige voorzitters van de auditcommissie hebben voorafgaand aan elke commissievergadering apart overleg met de lead auditpartner. Dat biedt gelegenheid om de agenda door te nemen en van de externe accountant te horen welke onderwerpen en vragen er op de vergadering aan de orde zouden moeten komen. De externe accountant kan ook vertellen wat er in

Vragen voor de private session met de externe accountant

- Hebt u aanbevelingen gedaan voor aanpassingen in de jaarrekening of in persberichten die niet zijn overgenomen? Indien dat het geval is, op welk gebied en van welke aard waren de door u gesuggereerde aanpassingen?
- Welke onderdelen van onze financiële verslaglegging zouden volgens u onderwerp van onderzoek door de toezichthouders kunnen zijn?
- Wat is volgens u de kwaliteit van onze gerapporteerde inkomsten in de huidige periode?
- Wat is uw beeld van de toon aan de top en die van de managers daaronder?
- Hoe capabel is ons financeteam?
- Is er volgens u sprake van druk die wordt uitgeoefend op personen binnen de verslagleggingsafdeling om tot een bepaalde uitkomst te komen, als het aankomt op specifieke boekhoudkundige zaken?
- Bent u van mening dat het management adequaat heeft opgetreden tegen personen die frauduleus of dubieus gedrag hebben vertoond?
- Zijn er zaken die u zorgen baren aangaande de wijze waarop de organisatie te werk gaat?
- Welke onderwerpen van de controle kosten het meeste tijd, veroorzaken overschrijdingen van het budget of leiden tot herhaaldelijke discussies met het management?
- Welke vragen zouden we u of het management moeten stellen? Waar moeten we meer tijd aan spenderen?
- In welke mate worden de presentaties aan de auditcommissie gerepeteerd en uitgeschreven?

de financiële kolom en andere geledingen van de organisatie speelt. Vaak wordt er ook na afloop van de vergadering nog even nabesproken.

‘Mini-heisessie’

Naast het overleg voorafgaand en na afloop van de reguliere vergadering, kan de voorzitter van de auditcommissie één keer per jaar een ‘mini-heisessie’ met de externe accountant organiseren: zonder formele agenda en ‘met de benen op tafel’, zonder notulen. In dat informele overleg kunnen de voorzitter van de auditcommissie en de lead auditpartner hun beeld, indrukken van en gevoel bij de organisatie aan elkaar toetsen en hun observaties en zorgen delen, bijvoorbeeld over de kwaliteit van het bestuur en de verhoudingen daarbinnen, de (financiële) organisatie en belangrijke issues als kwaliteit, langetermijnwaardecreatie, cultuur en integriteitsrisico’s. Commissarissen zijn vaak eenzaam in de uitoefening van hun rol: ze hebben veelal niemand die als spiegel en sparringpartner kan fungeren met betrekking tot de organisatie.

Uit de praktijk

De informele informatie-uitwisseling tijdens de **private session** kan ook worden geïnstitutionaliseerd. De auditcommissie van een beursgenoteerde organisatie houdt één keer per jaar een informele sharingmeeting met de externe accountant. Ter voorbereiding van de sessie doet de accountant een **deep dive** in de organisatie: hoe wordt er organisatiebreed, dus ook in de internationale vestigingen, tegen de financefunctie aangekeken, ook door de componentauditors (de lokale accountants die de controle van buitenlandse bedrijfsonderdelen uitvoeren in opdracht van de groepsauditor)? De externe accountant deelt de verzamelde indrukken met de auditcommissie, die op haar beurt de eigen zorgen over de financefunctie uit: waar bevinden zich gevaarlijke zwakke plekken in de financiële kolom en is er voldoende talent aanwezig in de top-20 om straks de opvolging van de zittende cfo soepel intern te kunnen opvangen? Het levert een vruchtbare informatie-uitwisseling op, omdat er sprake is van een veilige omgeving, waarin een sfeer heerst van wederzijds vertrouwen en de openheid van twee kanten komt.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

A. De relatie met Internal Audit

1. Rolinvulling en mandaat
2. Mensen, middelen en competenties
3. Scope en missie
4. Rapportage en opvolging
5. Evaluatie en beoordeling

B. De relatie met de externe accountant

1. Selecteren en voordragen voor benoeming
2. Beoordelen en bewaken van de onafhankelijkheid
3. Formuleren van de opdracht (scope, materialiteit en budget)
4. Communiceren met de externe accountant
5. Evalueren van het functioneren
Bijlagen

7. Corporate Reporting

8. Crisis

9. Communicatie

Veilige omgeving creëren voor indrukken en gevoelens

Een vruchtbare informele uitwisseling tijdens de **private session** komt niet uit zichzelf tot stand. De auditcommissie en de externe accountant bouwen daarvoor beide aan een sterke relatie. Zoals gezegd, zijn wederzijdse openheid en vertrouwen de belangrijkste bouwstenen van dat ‘bondgenootschap’. De vorming daarvan begint al bij de selectie, zoals we eerder schetsten. Dan al kan de auditcommissie aftasten of met de externe accountant een vertrouwensrelatie kan worden opgebouwd. Vervolgens kan de auditcommissie een omgeving creëren waarin de externe accountant zich veilig voelt om gevoelige kwesties te bespreken en zorgen te delen.

Tips en spelregels voor een veilige omgeving

- Wees alert op en reageer op non-verbale communicatie aan de kant van de externe

accountant: welke zorgen leven er onder de oppervlakte?

- Creëer een open sfeer, waarin indrukken en gevoelens bespreekbaar zijn.
- Bedenk van tevoren welke vragen de auditcommissie aan de externe accountant wil stellen: over welke gevoelige onderwerpen wil de auditcommissie de mening van de externe accountant horen of informele informatie verkrijgen (zie kader)?
- Ga zorgvuldig om met de verkregen informatie door voorzichtig te polsen bij het bestuur of Internal Audit, klap **nóóit** uit de school en bescherm de bron.
- Wees als auditcommissie ook **zélf** bereid om vertrouwelijke en gevoelige informatie met de externe accountant te delen, die ten goede kan komen aan de kwaliteit van de controle.
- Zoek, binnen of buiten de organisatie, een neutrale omgeving om het gewenste gesprek te faciliteren.

Uit de praktijk

De lead auditpartner van een organisatie merkt dat de slechte relatie tussen de ceo en de cfo op het punt staat om te exploderen. Hij belt de voorzitter van de auditcommissie om deze op de hoogte te stellen. Formeel is dat niet zijn rol, maar hij maakt zich zorgen. Na het telefoontje van de externe accountant belt de voorzitter van de auditcommissie, de president-commissaris die op zijn beurt direct contact opneemt met de ceo: ‘Wat hoor ik nu van de externe accountant?’ De in vertrouwen verstrekte informatie keert zich vervolgens als een boemerang tegen de lead auditpartner. Voortaan zal hij zich wel drie keer bedenken voor hij een gevoelig issue bij de voorzitter van de auditcommissie aankaart. Daarvoor is een veilige omgeving nodig, waarin gedeelde informatie binnenskamers blijft. Als die omgeving vijandig blijkt, klapt de externe accountant dicht en blijven de raad van commissarissen en de auditcommissie verstoken van belangrijke informele informatie.



5. Evaluatie van het functioneren van de externe accountant

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

De auditcommissie moet de wettelijke controle door de externe accountant monitoren. Bovendien rapporteert de auditcommissie jaarlijks aan de gehele raad van commissarissen over het functioneren van en de relatie met de externe accountant. Hoe kan de auditcommissie deze jaarlijkse evaluatie praktisch aanpakken en ervoor zorgen dat de uitkomst de meerwaarde van de externe accountant voor de auditcommissie vergroot?

Een algemeen uitgangspunt is dat de auditcommissie eigen beoordelingscriteria opstelt. Voor de auditcommissie zijn immers andere zaken belangrijk dan voor het bestuur, dat bij de beoordeling vooral kijkt naar de relatie van de externe accountant met het (lokale) management. Voor de auditcommissie zijn echter vooral zaken belangrijk als een onafhankelijke opstelling, professioneel scepticisme en een rechte rug. De auditcommissie kan dus niet aansluiten bij een bestaande evaluatie, maar zal een eigen beoordelingsproces opzetten.

- Best practices voor het evaluatieproces van de externe accountant**
- Schakel voor het jaarlijkse evaluatieproces (het hoofd) Internal Audit in.
 - Stel samen met de accountant vooraf relevante kwaliteitsindicatoren vast en betrek deze in het evaluatieproces.
 - Zorg dat de auditcommissie invloed heeft op de inhoud van de vragenlijsten.
 - Baken de scope af van de gewenste feedback en

- zorg dat de vragenlijst alleen wordt ingevuld door relevante stakeholders.
- Vul als voorzitter en leden van de auditcommissie ook zelf de vragenlijst in.
 - Weeg eventuele kritiek op de externe accountant op passende wijze. Kritiek of

- Maatschappelijk debat over de kwaliteit van de accountantscontrole**
- De maatschappelijke discussie over hoe de wettelijke accountantscontrole duurzaam verbeterd kan worden, wordt in binnen- en buitenland sinds enkele jaren steeds prominenter gevoerd. Belangrijke thema's die spelen voor de accountancysector:
- 1) eindrapport van de Kwartiermakers toekomst accountancy **Druk en Tegendruk**;
 - 2) implementatie van de Wijzigingswet accountancysector;
 - 3) implementatie van de Corporate Sustainability Reporting Directive (CSRD).

- Eindrapport Kwartiermakers**
- Eind 2023 kwamen de twee Kwartiermakers toekomst accountancy – aangesteld door de minister van Financien – met hun eindrapport **Druk en Tegendruk**. Het rapport werd afgesloten met een lijst aanbevelingen voor diverse stakeholders in de sector: van individuele accountant tot de toezichthouder.

- weerstanden in de organisatie kunnen namelijk zowel iets zeggen over de accountant als over de organisatie zelf.
- Stel samen met de accountant een actieplan op om de uitkomsten te evalueren en houd de overige leden van de raad op de hoogte van de voortgang.

- Deze aanbevelingen betroffen de onderwerpen fraude, kwaliteitsindicatoren, cultuur, innovatie, opleiding en structuurmodellen. Het is belangrijk dat de sector transparant maakt hoe er voortgang met de opvolging van deze aanbevelingen wordt gemaakt.
- Wijzigingswet accountancysector**
- Eind 2023 is de Wijzigingswet accountancysector naar de Tweede Kamer gestuurd voor behandeling. Hierin zit een aantal belangrijke elementen:
- i) verplichting voor accountantsorganisaties om te rapporteren op kwaliteitsindicatoren;
 - ii) aanwijsbevoegdheid voor de NBA (toewijzing van een accountantsorganisatie);
 - iii) uitbreiding aantal accountantsorganisaties met een onafhankelijke rvc;
 - iv) verduidelijking doel stelsel van kwaliteitsbeheersing. Op dit moment is het onduidelijk wanneer deze wijzigingswet wordt geagendeerd in de Tweede Kamer.

Betrek en bespreek in het evaluatieproces van de externe accountant ook de uitkomsten van AFM-onderzoeken naar de kwaliteit van de accountantscontrole. Na de evaluatie licht de raad van commissarissen de externe accountant in over de belangrijkste uitkomsten.

- Corporate Sustainability Reporting Directive**
- In november 2022 nam de Europese Unie de Corporate Sustainability Reporting Directive (CSRD) aan. Volgens deze richtlijn moeten steeds meer bedrijven vanaf 2024 verplicht rapporteren over de impact van hun activiteiten op mens en milieu. Hierbij is assurance verplicht.

Inmiddels – door politieke veranderingen in Europa – leidt de invoering van de CSRD tot meer discussie. De Europese Commissie kijkt op dit moment naar een totaalpakket (Omnibus) dat tot doel heeft de regeldruk voor bedrijven te verminderen en overlappingsen/ tegenstrijdigheden in de vereisten voor duurzaamheidsrapportage weg te nemen.

Bijlagen

Bijlage 6A	Overzicht van taken en verantwoordelijkheden voor de relatie met de externe accountant
Bijlage 6B	Aandachtspunten voor het offerteproces
Bijlage 6C	Vragen voor de selectie van de externe accountant
Bijlage 6D	Specifieke onafhankelijkheidsregelgeving voor OOB's en EU PIE's

Bijlage 6A Overzicht van taken en verantwoordelijkheden voor de relatie met de externe accountant

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
 - A. De relatie met Internal Audit
 1. Rolinvulling en mandaat
 2. Mensen, middelen en competenties
 3. Scope en missie
 4. Rapportage en opvolging
 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 1. Selecteren en voordragen voor benoeming
 2. Beoordelen en bewaken van de onafhankelijkheid
 3. Formuleren van de opdracht (scope, materialiteit en budget)
 4. Communiceren met de externe accountant
 5. Evalueren van het functioneren
7. Corporate Reporting
8. Crisis
9. Communicatie

Wettelijke taken van de auditcommissie volgens artikel 2 lid 2 Besluit instelling auditcommissie:

- het monitoren van de wettelijke controle van de jaarrekening en de geconsolideerde jaarrekening, in het bijzonder de uitvoering van de controle met inachtneming van de beoordeling van de AFM;
- het beoordelen en monitoren van de onafhankelijkheid van de externe accountant, waarbij met name wordt gelet op de verlening van nevendiensten aan de rechtspersoon;
- het vaststellen van de procedure voor de selectie van de externe accountant en de voordracht tot verlening van de opdracht tot het verrichten van de wettelijke controle.

Wettelijke taak (niet opgenomen in het Besluit instelling auditcommissie) van de auditcommissie volgens de EU-Auditverordening:

- selectie van de externe accountant door middel van een aanbestedingsprocedure.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

A. De relatie met Internal Audit

B. De relatie met de externe accountant

Taken en verantwoordelijkheden van de auditcommissie voor de relatie met de externe accountant

Principe 1.6 Benoeming en beoordeling van het functioneren van de externe accountant

De raad van commissarissen doet de voordracht tot benoeming van de externe accountant aan de algemene vergadering en houdt toezicht op het functioneren van de externe accountant.

1.6.1 Functioneren en benoeming

De auditcommissie rapporteert jaarlijks aan de raad van commissarissen over het functioneren van en de ontwikkelingen in de relatie met de externe accountant. De auditcommissie geeft advies aan de raad van commissarissen over de voordracht van de benoeming of herbenoeming dan wel het ontslag van de externe accountant en bereidt de selectie van de externe accountant voor. Bij voornoemde werkzaamheden betreft de auditcommissie de observaties van het bestuur. Mede op grond hiervan bepaalt de raad van commissarissen zijn voordracht aan de algemene vergadering tot benoeming van de externe accountant.

1.6.2 Informeren van de externe accountant over het functioneren

De raad van commissarissen licht de externe accountant op hoofdlijnen in over de rapportages omtrent zijn functioneren.

1.6.3 Opdracht

De auditcommissie doet een voorstel aan de raad van commissarissen voor de opdracht voor controle van de jaarrekening aan de externe accountant. Het bestuur faciliteert dit. Bij het formuleren van de opdracht is aandacht voor de reikwijdte van het accountantsonderzoek, de te hanteren materialiteit en

het honorarium van het accountantsonderzoek. De raad van commissarissen stelt de opdracht vast.

1.6.4 Verantwoording

De belangrijkste conclusies van de raad van commissarissen over de voordracht en de uitkomsten van het selectieproces van de externe accountant worden aan de algemene vergadering meegedeeld.

1.6.5 Vertrek van de externe accountant

De vennootschap publiceert een persbericht bij een tussentijds beëindiging van de relatie met de externe accountantsorganisatie. In het persbericht wordt de reden van de tussentijdse beëindiging toegelicht.

Principe 1.7 Uitvoering werkzaamheden door de externe accountant

De auditcommissie bespreekt met de externe accountant het controleplan en de bevindingen van de externe accountant naar aanleiding van zijn uitgevoerde werkzaamheden. Het bestuur en de raad van commissarissen onderhouden reguliere contacten met de externe accountant.

1.7.1 Informatievoorziening aan de externe accountant

Het bestuur draagt er zorg voor dat de externe accountant tijdig alle informatie ontvangt die nodig is voor de uitvoering van zijn werkzaamheden. Het bestuur stelt de externe accountant in de gelegenheid om op de verstrekte informatie te reageren.

1.7.2 Controleplan en bevindingen externe accountant

De externe accountant bespreekt het conceptcontroleplan met het bestuur, alvorens het aan de auditcommissie voor te leggen. De auditcommissie bespreekt jaarlijks met de externe accountant:

i. de reikwijdte en materialiteit van het auditplan en de belangrijkste

risico's van de jaarverslaggeving die de externe accountant heeft benoemd in het controleplan; en

ii. mede aan de hand van de daaraan ten grondslag liggende documenten, de bevindingen en de uitkomsten van de controlewerkzaamheden bij de jaarrekening en de management letter.

1.7.3 Publicatie financiële berichten

De auditcommissie beoordeelt of, en zo ja op welke wijze de externe accountant wordt betrokken bij de inhoud en publicatie van financiële berichten anders dan de jaarrekening.

1.7.4 Overleg met de externe accountant buiten aanwezigheid van het bestuur

De auditcommissie overlegt zo vaak als zij dit noodzakelijk acht, maar ten minste eenmaal per jaar, buiten aanwezigheid van het bestuur met de externe accountant.

1.7.5 Inzage discussiepunten tussen de externe accountant en het bestuur

De raad van commissarissen krijgt inzage in de belangrijkste discussiepunten tussen de externe accountant en het bestuur naar aanleiding van de concept management letter dan wel het concept accountantsverslag.

1.7.6 Aanwezigheid van de externe accountant bij de vergaderingen van de raad van commissarissen

De externe accountant woont in ieder geval de vergadering van de raad van commissarissen bij waarin het verslag van de externe accountant van het onderzoek van de jaarrekening wordt besproken (bron: Corporate Governance Code 2022).

146 | PwC Waarde toevoegen in tijden van verandering

<

<•

≡

>

Bijlage 6B Aandachtspunten voor het offerteproces

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances

A. De relatie met Internal Audit

1. Rolinvulling en mandaat

2. Mensen, middelen en competenties

3. Scope en missie

4. Rapportage en opvolging

5. Evaluatie en beoordeling

B. De relatie met de externe accountant

1. Selecteren en voordragen voor benoeming

2. Beoordelen en bewaken van de onafhankelijkheid

3. Formuleren van de opdracht (scope, materialiteit en budget)

4. Communiceren met de externe accountant

5. Evalueren van het functioneren

Bijlagen
7. Corporate Reporting
8. Crisis
9. Communicatie

Component	Doel(en)	Tip
1. Doelstellingen formuleren	• Focus in het offerteproces (opdrachtformulering). • Motivatie om het offerteproces tot een goed einde te brengen.	• Formuleer doelstellingen SMART (specifiek, meetbaar, acceptabel, realistisch, tijdgebonden).
2. Selectiecriteria vaststellen	• Helderheid over de boordeling van de inschrijvers. • Goede weergave van alle wensen en eisen van stakeholders. • Leidraad voor de evaluatie met de individuele inschrijvers.	• Standaardselectiecriteria resulteren in een standaardantwoord. Stel daarom selectiecriteria vast die gaan over de meerwaarde van, bijvoorbeeld, de aanpak of het team van de inschrijver. • Besteed aandacht aan harde en zachte selectiecriteria en aan de balans daartussen. • Stel niet te veel criteria op, dat leidt tot minder focus.
3. Medewerkers erbij betrekken	• Belangen van alle stakeholders behartigen. • Duidelijkheid over rollen en verwachtingen.	• Beperk het aantal betrokken medewerkers, anders kan het proces onnodig log worden. • Waak voor een te grote bestuurlijke vertegenwoordiging. • Betrek vooral ook operationeel management erbij.
4. Bepalen welke dienstverleners worden uitgenodigd	• Aanbestedingsprocedure vaststellen (indien OOB). • De passende dienstverleners uitnodigen.	• Stel realistische criteria voor de uitnodiging vast. • Communiceer tijdens het proces duidelijk over de regels en afspraken.
5. Planning en communicatie bepalen	• Inschatten van de tijd die het proces kost. • Vaststellen van de stappen die moeten worden doorlopen en de volgorde waarin dat moet. • Onduidelijkheid tijdens het proces voorkomen door heldere communicatie en alle inschrijvers gelijke kansen bieden.	• Begin tijdig met de planning en communicatie rondom het offerteproces.
6. De schriftelijke offertes beoordelen	• Zeker stellen dat de schriftelijke offerte voldoet aan de selectiecriteria.	• Gebruik een beoordelingsformulier om tot een volledige en zo veel mogelijk geobjectiveerde beoordeling te komen. • Bepaal wie de uiteindelijke beslissing neemt.
7. Presentatieronde houden	• Ervaren welke inschrijver het beste bij de organisatie past. • Toelichting op de geschreven offerte mogelijk maken.	• Geef duidelijke richtlijnen over de vorm en inrichting van de presentatie. • Voorkom onduidelijkheid over de beoordelingscriteria.
8. Evalueren	• Organiseren van feedback- en leermoment voor de inschrijvers en voor de organisatie.	• Voorkom onduidelijkheid over de argumenten voor uw keuze.

Bijlage 6C Vragen voor de selectie van de externe accountant

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

A. De relatie met Internal Audit

- 1. Rolinvulling en mandaat
- 2. Mensen, middelen en competenties
- 3. Scope en missie
- 4. Rapportage en opvolging
- 5. Evaluatie en beoordeling

B. De relatie met de externe accountant

- 1. Selecteren en voordragen voor benoeming
- 2. Beoordelen en bewaken van de onafhankelijkheid
- 3. Formuleren van de opdracht (scope, materialiteit en budget)
- 4. Communiceren met de externe accountant
- 5. Evalueren van het functioneren

Bijlagen

7. Corporate Reporting

8. Crisis

9. Communicatie

Het accountantskantoor en het team

- Geeft het team er blijk van onze organisatie en complexiteit goed te (willen leren) kennen?
- Heeft het team zich voldoende verdiept in de organisatie en haar omgeving voor een op maat gesneden offerte?
- Levert het accountantskantoor kwalitatief hoogstaande controlediensten in alle geografische gebieden waar we actief zijn?
- Sluiten de kernwaarden van het accountantskantoor aan op de kernwaarden van onze organisatie?
- Beschikt het kantoor over de passende sectorexpertise?
- Waaruit blijkt enthousiasme en **eagerness** van de voorgestelde teamleden voor de controle van de jaarrekening bij onze organisatie?
- Geeft het kantoor er blijk van gericht te zijn op samenwerking, uiteraard met behoud van zijn onafhankelijke rol?
- Beschikt het kantoor over specialisten op het gebied van bijvoorbeeld belastingen, treasury, corporate finance, IT-systemen en duurzaamheidsverslaggeving (CSRD); hoe en wanneer worden die ingezet in de controle van onze jaarrekening?
- Zijn de voorgestelde kernteamleden ervaren in de sector?
- Zijn de voorgestelde kernteamleden voldoende ervaren en gekwalificeerd?
- Geven de voorgestelde kernteamleden blijk van hoge professionele standaarden en persoonlijke integriteit?
- Geeft het accountantsteam ons (auditcommissie, bestuur, financiële functie) vertrouwen dat we een accountantscontrole van goede kwaliteit zullen krijgen?
- Hoe is de continuïteit van de teambezetting geborgd? Hoe gaat het kantoor om met eventueel roulatie en vertrek van teamleden?
- Hoe heeft het accountantskantoor geborgd dat wordt voldaan aan de (lokale) regelgeving op het vlak van onafhankelijkheid van de externe accountant? Hoe houdt de groepsaccountant hier grip op in de verschillende landen?
- Op welke wijze denkt de accountant invulling te gaan geven aan zijn/haar natuurlijke adviesfunctie? Wat verwachten wij als auditcommissie en bestuur van die natuurlijke adviesfunctie?
- Hoe denkt het controleteam te kunnen bijdragen aan het lerend vermogen van onze organisatie en de financiële functie en risicomanagementfunctie in het bijzonder?
- Wanneer, op welke wijze en aan wie vraagt het accountantsteam om feedback op zijn eigen functioneren?

Controleaanpak

- Is de controleaanpak op maat gesneden voor onze organisatie?
- Houdt het controleplan rekening met specifieke kenmerken van onze organisatie, onze cultuur, onze activiteiten en voornaamste risico's?
- Wat is de voorgestelde reikwijdte (scope) van de controle? Sluit die reikwijdte aan op de verwachtingen van de auditcommissie en het bestuur?
- Welke materialiteit hanteert de accountant in zijn controle? Sluit die materialiteit aan bij de verwachting van de auditcommissie?
- Waaruit blijkt dat in de controleaanpak rekening is gehouden met eventuele specifieke wensen van de auditcommissie en/of het bestuur?
- Op welke wijze besteedt de accountant aandacht aan cultuur en gedrag en hoe wordt daarover gecommuniceerd?
- Hoe gaat er door de externe accountant samengewerkt worden met Internal Audit? Hoe kijkt Internal Audit daar tegenaan?
- Aan wie en op welk moment stelt de externe accountant voor om verslag van zijn of haar werkzaamheden uit te brengen?
- Wat stelt het team voor te bespreken met de auditcommissie en wanneer in de tijd vinden die besprekingen plaats?
- Op welke wijze is in de controleaanpak voorzien in private sessions van de externe accountant met de auditcommissie?
- Sluit de planning van de accountant aan op onze eigen planning-en-controlcyclus en de timing van de externe informatievoorziening?
- Op welke wijze wordt in de controle aandacht besteed aan frauderisico's?
- Hoe wordt de auditcommissie geïnformeerd in geval van (vermoedens) van misstanden of fraude?
- Is het controlehonorarium een faire vergoeding voor een accountantscontrole met de voorgestelde reikwijdte en materialiteit?
- Hoe kijkt de externe accountant aan tegen het eventueel publiekelijk maken van de punten uit de interim-bevindingen van de rapportage en/of het accountantsverslag?
- Hoe kijkt de externe accountant aan tegen het verstrekken van informatie en beantwoorden van vragen op de aandeelhoudersvergadering?
- Op welke wijze worden in de controleaanpak moderne digitale controletechnieken zoals data-analyse en kunstmatige intelligentie toegepast?
- Op welke randvoorwaarden en uitgangspunten (zoals ten aanzien van het niveau van de interne beheersing en de kwaliteit van oplevering van documenten) zijn het controleplan en het controlehonorarium gebaseerd?

Bijlage 6D Specifieke onafhankelijkheidsregelgeving voor OOB's en EU PIE's

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
 - A. De relatie met Internal Audit
 - 1. Rolinvulling en mandaat
 - 2. Mensen, middelen en competenties
 - 3. Scope en missie
 - 4. Rapportage en opvolging
 - 5. Evaluatie en beoordeling
 - B. De relatie met de externe accountant
 - 1. Selecteren en voordragen voor benoeming
 - 2. Beoordelen en bewaken van de onafhankelijkheid
 - 3. Formuleren van de opdracht (scope, materialiteit en budget)
 - 4. Communiceren met de externe accountant
 - 5. Evalueren van het functioneren
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie

Nieuw in de EU-onafhankelijkheidsregels is dat er sprake is van een afkoelingsperiode van een jaar met betrekking tot de door de te benoemen externe accountant geleverde diensten op het gebied van **designing and implementing internal control or risk management procedures related tot the preparation and/or control of financial information or financial information technology systems**. De externe accountant kan niet worden benoemd als deze dergelijke diensten heeft verleend in het jaar voorafgaand aan het eerste door hem te controleren boekjaar.

Met betrekking tot OOB's/EU PIE's zijn de verantwoordelijkheden van de auditcommissie (en van de externe accountant) op het gebied van de onafhankelijkheid bij de invoering van de EU PIE-regelgeving meer expliciet gemaakt en uitgebreid. Ook de rapportage door de externe accountant aan de auditcommissie is meer gedetailleerd geworden. Zo moet de externe accountant bevestigen dat, indien bij de controle van de OOB-jaarrekening gebruik is gemaakt van andere niet aan het netwerk van de externe accountant verbonden accountants of experts, deze hun onafhankelijkheid ten opzichte van de onderneming aan de externe accountant hebben bevestigd.

Naast het vaststellen (dan wel updaten) van het eigen ondernemingsbeleid ten aanzien van het door de externe accountant mogelijk uitvoeren van wettelijk toegestane niet-controledienstverlening, moet de auditcommissie alle wettelijk toegestane en door de onderneming gewenste niet-

controledienstverlening vooraf goedkeuren¹. Daarbij moet de auditcommissie de eventuele bedreigingen van de onafhankelijkheid en de door de externe accountant getroffen maatregelen om deze bedreigingen tot een acceptabel niveau terug te brengen in haar afwegingen betrekken².

Een Nederlandse externe accountant mag geen andere diensten dan (de wettelijk vastgelegde) 'controlediensten' verlenen aan de Nederlandse OOB, de moedermaatschappij(en) van de OOB, dan wel aan in de EU gevestigde dochtermaatschappijen van de OOB (meer dan 50% zeggenschap). Buitenlandse netwerkfirma's verbonden aan de externe accountant mogen aan in Nederland gevestigde groepsmaatschappijen ook alleen 'controlediensten' verlenen. Aan in het buitenland gevestigde groepsmaatschappijen (meer dan 50% zeggenschap) mogen zij niet-controlediensten verlenen, indien en voor zover deze toegestaan zijn onder de in het land van vestiging geldende onafhankelijkheidsregels. (NB: de onafhankelijkheidsregelgeving voor EU OOB's kan van land tot land verschillen. Het is daarom van groot belang om vast te stellen dat een bepaalde dienst inderdaad is toegestaan in de EU-lidstaat, waar de desbetreffende dochteronderneming is gevestigd.) De auditcommissie moet ook richtlijnen opstellen voor het inhuren van de externe accountant voor bepaalde belastingadvieswerkzaamheden (waaronder aangiftewerkzaamheden ten behoeve van de onderneming) en waarderingsdiensten ten behoeve van groepsmaatschappijen in EU-lidstaten waar dat onder voorwaarden is toegestaan.

De externe accountant van een OOB (EU PIE) moet jaarlijks in de accountantsverklaring vermelden dat er gedurende het boekjaar geen EU-verboden diensten aan de onderneming zijn verleend. Om dit statement te kunnen maken en om te voorkomen dat er onverhoopt toch 'verboden diensten' worden verleend, is het een gezamenlijke verantwoordelijkheid van de externe accountant en de onderneming/auditcommissie om te beschikken over een adequaat werkende procedure van voorafgaande goedkeuring, ten aanzien van te leveren niet-controlediensten.

Voor OOB's geldt bovendien een honorariumplafond van 70% van de gemiddelde honoraria voor de wettelijke controle als bovengrens voor de door de externe accountant van de OOB te leveren andere diensten³.

Met betrekking tot OOB's moet de externe accountant de diensten die door de externe accountant zijn verleend aan de onderneming anders dan de wettelijke controle, in zijn accountantsverklaring vermelden, tenzij deze al door de onderneming zijn opgenomen in het jaarverslag of de jaarrekening.



¹ Indien er sprake is van dienstverlening aan een dochteronderneming, die zelf ook een auditcommissie heeft, geldt de verplichting van voorafgaande goedkeuring voor beide auditcommissies; dit is met name het geval bij banken en verzekeraars.
² Het is toegestaan om voor bepaalde categorieën diensten, bijvoorbeeld een 'totaalbedrag' vooraf goed te keuren, zodat niet voor elke individuele kleine opdracht apart goedkeuring hoeft te worden gegeven.
³ In de Nederlandse situatie heeft het honorariumplafond naar verwachting niet veel praktische betekenis, gezien het totaalverbod op het leveren van andere diensten dan 'controlediensten' aan OOB's. Voor de dienstverlening aan Europese dochtermaatschappijen van Nederlandse banken en verzekeraars is het honorariumplafond wel van belang, omdat deze Europese dochters zelf ook EU PIE zijn; het honorariumplafond moet dan worden berekend voor elke afzonderlijke EU PIE.



Corporate Reporting

Kwaliteit en integriteit van de verslaggeving

07

7. Corporate Reporting

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekening
- 8. Crisis
- 9. Communicatie

Transparantie en verantwoording zijn kernbegrippen van goed bestuur. Stakeholders hebben recht op tijdige, juiste, volledige en waarheidsgetrouwe informatie over het gevoerde beleid en de waardecreatie van de organisatie in het jaarverslag en de interimrapportages op zowel de korte, middellange als lange termijn. De auditcommissie speelt een centrale rol in het toezicht op de integriteit en kwaliteit van de financiële (en niet-financiële) verslaggeving.

Het is een van de allerbelangrijkste verantwoordelijkheden van de auditcommissie: het monitoren van de financiële en niet-financiële verslaggeving, als ondersteuning van het toezicht daarop door de raad van commissarissen. De auditcommissie richt zich daarbij primair op de kwaliteit, integriteit en transparantie van de informatie in het jaarverslag en in de interim-rapportages (zoals halfjaar- en kwartaalcijfers en persberichten). De auditcommissie beoordeelt ook of de financiële en niet-financiële informatievoorziening in lijn is met de **purpose** en de waarden van de organisatie. Zie daarvoor ook hoofdstuk 3: Corporate impact.

Stakeholders moeten erop kunnen vertrouwen dat het bestuur hen tijdig, correct en volledig informeert en dat de informatie een getrouw beeld van de werkelijkheid vormt. Aandeelhouders baseren zich op deze informatie voor hun (des)investeringsbeslissing, beurskoersen kunnen erdoor beïnvloed worden.

Financiers, kapitaalverstrekkers en (potentiële) medewerkers beschouwen de informatie als een waarborg voor de continuïteit, die de belangrijkste voorwaarde voor de samenwerking vormt. De maatschappij gebruikt de informatie om te bepalen of de organisatie een licence to operate verdient.

De rol van de auditcommissie

Gehele verslaggevings- en auditproces overzien

Bij de monitoring richt de auditcommissie zich op het gehele verslaggevingsproces. Dat begint met het permanent beoordelen van de interne risicobeheersings- en controlesystemen: zorgen de rapportagelijnen ervoor dat alle managementlagen en (internationale) bedrijfsonderdelen de financiële en niet-financiële informatie correct en compleet en ook nog eens op tijd en op consistente wijze aanleveren? Daarnaast houdt de auditcommissie zich bezig

met de beoordeling van de jaarrekening en niet-financiële verantwoording: is deze juist, volledig en waarheidsgetrouw? Verder monitort de auditcommissie de wettelijke controle door de externe accountant en het resultaat daarvan voor de kwaliteit en de integriteit van de verslaggeving. De auditcommissie beoordeelt ook de effectiviteit van het interne en externe auditproces en ziet erop toe of het bestuur de aanbevelingen en opmerkingen van Internal Audit en de externe accountant naleeft en opvolgt. De auditcommissie brengt daarover verslag uit aan de raad van commissarissen en legt ook verantwoording af in het jaarverslag (als onderdeel van het verslag van de raad van commissarissen).

In dit hoofdstuk komen de volgende onderwerpen aan de orde:

- 1. Beoordelen van de financiële verslaggeving (jaarrekening)
- 2. Beoordelen van het bestuursverslag
- 3. Beoordelen van de financiële informatie buiten de jaarrekening



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekeningBijlagen
- 8. Crisis
- 9. Communicatie

Assurance over duurzaamheidsrapportage

Het huidige wetsvoorstel van de Europese Commissie met betrekking tot de duurzaamheidsrapportage van ondernemingen (Corporate Sustainability Reporting Directive, CSRD), zal daarbij voor verslagen over kalenderjaar 2023 de auditcommissie belasten met bepaalde taken met betrekking tot assurance over de duurzaamheidsrapportage. Denk aan het in kennis stellen van de raad van commissarissen over de resultaten van assurance en de rol van de auditcommissie in dit proces, inclusief hoe de auditcommissie heeft bijgedragen aan de integriteit van de duurzaamheidsrapportage.



De wettelijke taken van de auditcommissie ten aanzien van de financiële verslaggeving

- het monitoren van het proces van financiële verslaggeving, plus het doen van voorstellen om de integriteit van het proces te waarborgen;
- het monitoren van de doeltreffendheid van het interne beheersingssysteem, het eventuele interne-auditsysteem en het risicomanagementsysteem met betrekking tot de financiële verslaggeving;
- het monitoren van de wettelijke controle van de (geconsolideerde) jaarrekening, plus (voor OOB's) het in overweging nemen van de bevindingen van de toezichthouder AFM;
- het informeren van de raad van commissarissen over het resultaat van de wettelijke controle: op welke wijze heeft deze bijgedragen aan de integriteit van de financiële verslaggeving en welke rol heeft de auditcommissie in dat proces gespeeld?

En:

- het beoordelen en monitoren van de onafhankelijkheid van de externe accountant, waarbij met name wordt gelet op de verlening van nevendiensten aan de rechtspersoon;
- het vaststellen van de procedure voor de selectie van de externe accountant en de voordracht tot verlening van de opdracht tot het verrichten van de wettelijke controle.

De twee laatste taken blijven hier onbesproken en komen uitgebreid aan de orde in hoofdstuk 6, deel II: De relatie met de externe accountant.



1. Beoordelen van de financiële en niet-financiële verslaggeving

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekeningBijlagen
- 8. Crisis
- 9. Communicatie

De interne risicobeheersings- en controle-systemen moeten een redelijke mate van zekerheid geven dat de financiële en niet-financiële verslaggeving geen onjuistheden van materieel belang bevat. Het bestuur is hiervoor verantwoordelijk.

■ De rol van de auditcommissie

Monitoren en versterken van het rapportageproces

De auditcommissie monitort de wijze waarop het bestuur invulling geeft aan het rapportageproces en is alert op risico's voor de kwaliteit en de integriteit van de verslaggeving. Bij geconstateerde onjuistheden kan het gaan om fouten (waarbij geen opzet in het spel is), maar ook om opzettelijke misleiding en fraude. Voor een uitgebreide bespreking van verslaggevings- en frauderisico's verwijzen we naar hoofdstuk 4: Risicobeheersing en interne controle.

Voorstellen voor waarborgen integriteit

De auditcommissie monitort niet alleen het proces van financiële verslaggeving, maar heeft volgens de wet ook de taak voorstellen te doen om de integriteit van het proces te waarborgen. Het is dus ook van belang dat de auditcommissie een eigen visie ontwikkelt op de versterking van de risicobeheersing en interne controle, om de betrouwbaarheid van de financiële en niet-financiële rapportage te bewaken of te vergroten en daarmee de kans op onjuistheden en fraude te verkleinen. Tegelijkertijd

moet de auditcommissie haar onafhankelijke positie waarborgen. De auditcommissie kan bijvoorbeeld aanbevelingen doen om de interne controle te versterken, maar houdt vervolgens ook onafhankelijk toezicht op de uitvoering. Het bestuur is uiteraard verantwoordelijk voor het invulling geven aan de risicobeheersing en interne controle en het continu verbeteren daarvan. De auditcommissie daagt het bestuur daarop uit. De auditcommissie kan voor het doen van concrete voorstellen input vragen van Internal Audit en de externe accountant: waar zitten volgens hen de zwakke plekken in het proces van verslaggeving?

Altijd op de agenda

De bespreking van de jaarrekening en de uitkomsten van de jaarrekeningcontrole met bestuur en externe accountant bevat in elk geval de volgende onderdelen:

- de keuze en toepassing van de (gewijzigde) grondslagen van waardering: zijn deze toereikend?;
- de belangrijkste schattingen;
- het proces van opstellen van jaarrekening en jaarverslag en **representations** van interne afdelingen (naast de externe accountant), zoals de **disclosure committee** (verantwoordelijk voor de monitoring van de juistheid en volledigheid van de informatie), legal, tax, treasury, et cetera, zodat de auditcommissie weet dat het **due process** is doorlopen en zij zich daarop kan en mag verlaten;
- financiering en – indien van toepassing – de onderbouwing door het bestuur van de **going concern**-assumptie;
- geconstateerde tekortkomingen in de risicobeheersing en interne controle.

Aanbevolen wordt om gedurende het jaar al relevante onderwerpen te bespreken, zoals:

- belangrijke grondslagaanpassingen;
- wijzingen en tekortkomingen in de risicobeheersing en interne controle;
- belangrijke transacties/gebeurtenissen met een significante impact op de jaarrekening.

Toezicht houden op de jaarrekening

Een van de hoofdtaken van de auditcommissie is het beoordelen van de jaarrekening op kwaliteit en integriteit. Geeft deze een getrouw beeld van de activiteiten en de positie van de organisatie in de verslagperiode? Daarbij kan de auditcommissie de volgende vragen stellen:

- Is de jaarrekening volledig en komt deze overeen met de informatie waarover de auditcommissie beschikt?
- Bevat de jaarrekening geen onjuistheden van materieel belang?
- Welke materiële overwegingen zijn gehanteerd?

- Zijn bij verslaggevingsissues de juiste oordelen gevormd en keuzes gemaakt en zijn deze conform recente uitspraken van regelgevende instanties, externe toezichthouders en beroepsorganisaties?
- Legt het bestuur transparant en op de juiste manier verantwoording af?
- Is de continuïteit voor de komende twaalf maanden (na het opstellen van het verslag) gewaarborgd?
- Is de jaarrekening opgesteld in overeenstemming met geldende verslagleggingsstandaarden?

De auditcommissie bespreekt de jaarrekening en de uitkomsten van de jaarrekeningcontrole met het bestuur en de externe accountant.

Discussie aangaan over integriteit

De beoordeling van de jaarrekening vraagt om de juiste expertise, gerijpte ervaring – bijvoorbeeld opgedaan in een financiële (bestuurs)functie of bij andere auditcommissies – een scherpe blik en de moed om een eerlijke discussie aan te gaan met het bestuur. Naast technische vragen over de kwaliteit van de rapportage, moet de auditcommissie ook de integriteit ervan toetsen, door zicht te krijgen op de toon aan de top ten aanzien van de rapportage.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen
8. Crisis
9. Communicatie

Vragen voor het bestuur over de jaarrekening (en de antwoorden)

Welke vragen stellen?	Aan wie?	Waarop letten in het antwoord?
Hoe heeft het bestuur de belangrijkste waarderingsgrondslagen, oordelen en schattingen bepaald en toegepast?	Bestuur	• Heeft het bestuur de belangrijkste beleidslijnen en schattingen geformuleerd? • Zijn deze in lijn met de kennis van de leden van de auditcommissies en de raad van commissarissen? • Zijn deze oordelen een goede representatie van de strategie van de organisatie?
Hoe gevoelig zijn omzet en resultaat voor minder positieve scenario's?	Bestuur	• Zijn de benoemde punten belangrijke aandachtspunten voor de organisatie? • Zijn de antwoorden in lijn met de kennis van de auditcommissie over de organisatie?
Zijn er issues geweest met betrekking tot de interne controle in relatie tot de totstandkoming van de jaarrekening?	Bestuur/externe accountant/ interne auditor	• Welke impact zouden deze issues kunnen hebben? • Hoe is hiermee omgegaan?
Welke alternatieve waarderingsgrondslagen zijn er door vergelijkbare organisaties gebruikt?	Bestuur/externe accountant	• Gebruikt de organisatie dezelfde grondslagen als vergelijkbare ondernemingen?
Wat is de impact van de risico's en kwetsbare punten voor de organisatie op de jaarrekening?	Bestuur	• Zijn de gevoeligheden duidelijk en gecommuniceerd?
Wat zijn de implicaties van verwachte veranderingen in waarderingsgrondslagen naar aanleiding van nieuwe verslaggevingsstandaarden en/of interpretaties?	Bestuur/externe accountant	• Zal de jaarrekening er significant anders uitzien?
Wat is de impact van de financieringsstructuur van de organisatie op de huidige en toekomstige winstgevendheid en hoe wordt hiermee omgegaan in het jaarverslag van de organisatie?	Bestuur	• Zijn de risico's met betrekking tot de financiering voldoende vastgesteld en benoemd?
Hoe nuttig en relevant is de overige informatieverstrekking, zoals continuïteitsissues?	Bestuur/externe accountant	• Zijn alle genoemde zaken logisch? • Komen de genoemde zaken voor wat betreft inhoud en toon overeen met de kennis die de auditcommissie heeft van de activiteiten van de organisatie? • Wat waren de grote aandachtspunten voor de organisatie in het afgelopen jaar en komen deze terug in de rapportages?
Zijn er indicatoren die duiden op fraude?	Bestuur/externe accountant	• Zijn deze indicatoren benoemd door het bestuur? • Is de impact hiervan geanalyseerd?

Zie bijlage 7A voor een uitgebreide lijst met vragen die de auditcommissie aan het bestuur kan stellen

Ontwijkende antwoorden? Doorvragen!

Hoewel de voorzitter en de leden van de auditcommissie streven naar een positieve relatie met het bestuur, gebaseerd op wederzijds vertrouwen, is het noodzakelijk dat ze tegelijkertijd een onafhankelijke geest en scepsis tentoonspreiden. Belangrijk hierbij is de bereidheid om het bestuur kritische vragen te stellen en dóór te vragen over ongemakkelijke onderwerpen, zoals frauderisico's en de subjectiviteit van de oordelen van het bestuur bij de totstandkoming van de jaarrekening. Het bestuur verwacht dat zelfs van de auditcommissie. Als de antwoorden ontwijkend of defensief zijn, is dat voor de auditcommissie een reden te meer om door te vragen.

Samenwerking met de externe accountant

De auditcommissie houdt toezicht op de wettelijke controle door de externe accountant. Samen bespreken zij de belangrijkste risico's van de jaarverslaggeving die zijn benoemd in het controleplan en de bevindingen en de uitkomsten van de controlewerkzaamheden bij de jaarrekening, in de rapportage van de interim-bevindingen en het accountantsverslag. In feite zijn de auditcommissie en de externe accountant 'bondgenoten': ze zien beide toe op de kwaliteit en de integriteit van de verslaggeving en kunnen elkaar daarin versterken. De externe accountant vormt bovendien een belangrijke onafhankelijke informatiebron voor de auditcommissie. Niet alleen voor de beoordeling van de jaarrekening, maar ook voor het toezicht op het bestuur.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving
 2. Beoordelen van het bestuursverslag
 3. Beoordelen van de financiële informatie buiten de jaarrekening
- Bijlagen

8. Crisis

9. Communicatie

Kritische vragen aan het bestuur over de integriteit van de financiële rapportage

- Welke transacties, schattingen en/of boekingen in de verslagperiode hebben een significante invloed op het resultaat dan wel de financiële ratio's?
- Worden gebruikelijke winstbegrippen gehanteerd, die aansluiten bij verslaggevingstandaarden, of worden zogenoemde alternatieve winstbegrippen gehanteerd, zoals EBITDA, gecorrigeerde EBITDA of resultaat voor bijzondere baten en lasten? Is het gehanteerde winstbegrip consistent met wat gebruikelijk is binnen de sector? Op welke wijze kan het management dit beïnvloeden? Worden op consistente wijze zowel de 'plussen' als de 'minnen' gecorrigeerd op het resultaat? En is er een goed onderbouwde reden voor wijziging van het winstbegrip?
- Zijn de gemaakte schattingen realistisch? En waarop zijn deze gebaseerd?
- Werden er in de laatste weken van de verslagperiode posten en transacties opgevoerd die niet eerder in de verslagperiode voorkwamen?
- Werden er belangrijke uitzonderingen gerapporteerd in de interne representation letters (bevestiging bij de jaarrekening) over de financiële verslaggeving, die werden ondertekend door verschillende managers door de organisatie heen?
- Welke afwegingen moesten er gemaakt worden tijdens de verslagperiode? Hoe zag het besluitvormingsproces eruit?
- Geeft het bestuur een heldere en onderbouwde toelichting waarom de resultaten afwijken van van de eerdere prognose?
- Welke inbreng in de toepassing van verslaggevingsgrondslagen heeft het niet-financiële management van de organisatie?
- Welke onderwerpen vormen steeds terugkerende uitdagingen of problemen?
- Als een journalist een artikel zou wijden aan de rapportage van de organisatie, waar zou dat dan waarschijnlijk over gaan?
- Waar liggen jullie 's nachts wakker van?
- Welke verslaggevingsonderwerpen kosten de meeste tijd van medewerkers in de financiële kolom?
- Welke factoren zetten de financiële rapportage onder druk?

Het wordt aanbevolen om deze vragen niet alleen te stellen bij het bespreken van de jaarrekening, maar ook al gedurende het verslagjaar.



Vragen over de jaarrekening aan de externe accountant

Best practice: bespreek vooraf met de externe accountant welke onderwerpen de auditcommissie graag terugziet in de rapportage van de interim-bevindingen of het accountantsverslag. Indien onderwerpen niet rechtstreeks in deze rapportages behandeld worden, dan kan de auditcommissie de volgende vragen stellen tijdens de bespreking hiervan:

- Wijkt de werkelijke reikwijdte van de controle af van die volgens het controleplan?
- Heeft het bestuur op enigerlei wijze de reikwijdte van de controle beperkt?
- Hebben het bestuur en het management tijdens de controle medewerking verleend en is de accountant voorzien van alle informatie en uitleg die nodig was, zonder terughoudendheid?
- Heeft het verkrijgen van schriftelijke verklaringen van het bestuur en het management problemen opgeleverd?
- Zijn er naar aanleiding van de controle belangrijke correcties in de jaarrekening aangebracht?
- Zijn er naar aanleiding van de controle niet-doorgevoerde correcties geweest?
- Welke onderdelen zijn het meest gevoelig voor subjectiviteit? Zijn de schattingen conservatief of agressief ingestoken en is dit in lijn met voorgaande jaren?
- Beschouwt de accountant de grondslagen voor de verslaggeving als voorzichtig of agressief?
- Heeft het bestuur zich verzet tegen het delen van belangrijke informatie?

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen

8. Crisis

9. Communicatie

Bepalen van de materialiteit

Materialiteit speelt een rol in financiële rapportages: wanneer is een verslaggevingsissue of een zwakte in de interne controle van materieel belang voor de verslaglegging? De gehanteerde materialiteitsdrempel bepaalt of deze tekortkomingen gemeld moeten worden en of er een noodzaak bestaat om de rapportage aan te passen, of zelfs om al gepubliceerde cijfers te corrigeren.

Kwantitatieve en kwalitatieve drempels

De meeste organisaties hanteren een vuistregel voor een kwantitatieve drempel voor materialiteit, bijvoorbeeld uitgedrukt in een percentage van het resultaat voor belasting. Voor halfjaar- en kwartaalrapportages kunnen andere drempels worden gehanteerd dan voor jaarresultaten. Naast een vuistregel die gebaseerd is op een kwantitatieve drempel, zijn er andere kwantitatieve aspecten waarmee rekening gehouden moet worden, zoals het voldoen aan bankconvenanten en – in bijvoorbeeld de bancaire wereld – eisen aan solvabiliteit of liquiditeit, die een impact kunnen hebben op de continuïteit van een organisatie.

Materialiteit heeft echter ook kwalitatieve aspecten, die zich niet of nauwelijks laten vangen in cijfermatige grenzen. Tekortkomingen in de interne controle, leidend tot onjuistheden of fraude in de jaarrekening, kunnen niet alleen de resultaten beïnvloeden, maar bijvoorbeeld ook schade toebrengen aan de reputatie van de organisatie. Dat vraagt om een ándere vuistregel:

Wanneer is een relatief kleine onregelmatigheid toch materieel?

Wees alert op boekhoudkundige fouten of onregelmatigheden, die het volgende – bedoelde of onbedoelde - effect kunnen hebben:

- maskeren van een negatieve trend in omzet, winstgevendheid of winst per aandeel;
- verbergen van onvermogen om tegemoet te komen aan de verwachtingen van analisten;
- veranderen van verlies in winst, of andersom;
- helpen verbergen van een illegale transactie, gepaard gaand met niet-integer handelen van het senior management;
- toenemen van de remuneratie, bijvoorbeeld door het alsnog bereiken van de prestatiedoelen voor variabele beloning;
- negatieve invloed op naleving van bankconvenanten, andere contractuele overeenkomsten of regelgeving.



informatie is materieel als deze het oordeel over de organisatie van belangrijke stakeholders beïnvloedt.

Ga de discussie aan: ligt de drempel van de auditcommissie lager?

Bij de bepaling van materialiteit wordt er dus rekening gehouden met zowel kwantitatieve als kwalitatieve aspecten. Bij die laatste speelt oordeelsvorming een belangrijke rol. Om de rapportage goed te kunnen beoordelen, is het belangrijk voor de auditcommissie om te weten welke drempel voor materialiteit het bestuur hanteert en hoe die is bepaald. De auditcommissie kan ook een eigen visie op materialiteit formuleren en de discussie aangaan wanneer haar drempel lager ligt dan die van het bestuur of wanneer bij de bepaling van de drempel andere aspecten belangrijk worden gevonden.

Afstemming met de externe accountant

Ook de externe accountant hanteert richtlijnen voor de materialiteit. Deze richtlijnen bepalen niet

alleen welke onderwerpen worden meegenomen in de controlewerkzaamheden, maar ook of en op welke punten de accountant voorstellen doet om tekortkomingen in de rapportage te corrigeren en of de auditcommissie daarvan op de hoogte wordt gebracht.

Wat wil de auditcommissie gerapporteerd krijgen?

De auditcommissie doet er verstandig aan om de gehanteerde materialiteit te bespreken met de externe accountant: zowel tijdens het selectieproces van de accountant als voorafgaand aan de controle. Op die manier kan worden ingeschat of het bestuur, de externe accountant en de auditcommissie op één lijn zitten. De auditcommissie kan ook aangeven waarvan ze op de hoogte wil zijn en wat ze gerapporteerd wil krijgen van de accountant, bijvoorbeeld álle voorgestelde aanpassingen, plus het al of niet overnemen daarvan door het bestuur.

Pas bij dynamiek ook materialiteit aan

Het bepalen van materialiteit is een dynamisch

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen

8. Crisis

9. Communicatie

Zicht krijgen op complexe en risicovolle posten en transacties in de jaarrekening

Een effectieve auditcommissie richt zich primair op de meest complexe en risicovolle posten en transacties in de financiële rapportage, waarbij oordeelsvorming een belangrijke rol speelt.

Vraag het bestuur en de accountant om een samenvatting

Omwille van de efficiency kan de auditcommissie het bestuur en/of de externe accountant vragen reliëf aan te brengen in de informatie. Zo kan de auditcommissie het bestuur vragen om een overzicht van de belangrijkste veranderingen en toevoegingen ten opzichte van de vorige verslagperiode, plus relevante ontwikkelingen (zoals de invoering van nieuwe regelgeving) die de verslaglegging hebben beïnvloed.

Waarop kan de auditcommissie speciaal letten in de jaarrekening?

- belangrijke afwijkingen van resultaten ten opzichte van voorgaande resultaten, of de prognose;
- complexe en/of ongebruikelijke transacties;
- terreinen waarbij oordeelsvorming een rol speelt, zoals schattingen en voorzieningen;
- in het bijzonder gebieden waarop andere veronderstellingen of oordelen een belangrijk effect op de jaarrekening zouden kunnen hebben. Voorbeelden: herstructureringskosten, overnames, verslaggeving van derivaten, waardering van activa, garantieverplichtingen, milieuverplichtingen of voorzieningen in verband met gerechtelijke procedures.

Best practice: een **issue tracker** kan een goed middel zijn om belangrijke thema’s gedurende het jaar te volgen.

De auditcommissie kan het bestuur ook vragen naar een samenvatting van de meest gevoelige of risicovolle thema’s in de verslagperiode.

Afwijkende resultaten

De auditcommissie is alert op afwijkingen in de rapportages over de verschillende verslagperioden. Welke verklaring heeft het bestuur voor de afwijkingen en voor belangrijke verschillen tussen de werkelijke resultaten en de budgetten of prognoses? Geeft de huidige financiële rapportage aanleiding tot het bijstellen van het beeld dat naar voren komt uit de jaarprognose/meerjarenprojecties? Een effectieve auditcommissie is ook alert op een significante verandering in de resultaten of plotselinge volumewisselingen (bijvoorbeeld omzet) vlak voor het eind van de verslagperiode.

Best practice

Wees alert op niet-standaardpassages in de bevestiging bij de jaarrekening van het management voor de externe accountant, zoals ongebruikelijke transacties of bijzondere gebeurtenissen in de verslagperiode. Vraag de externe accountant welke passages zijn toegevoegd aan de standaardbevestiging bij de jaarrekening, die doorgaans als bijlage aan het accountantsverslag wordt toegevoegd.

De auditcommissie zal in dat geval aan het bestuur vragen waarom de targets in het begin van het (half)jaar of kwartaal niet werden gehaald en aan het eind ineens wel. Andersom zal de auditcommissie het bestuur ook vragen waarom een (positieve) verandering van resultaten uitblijft, terwijl deze wel aannemelijk zou zijn, volgens de operationele of andere informatie waarover de auditcommissie beschikt.

Schattingen

Schattingen vereisen een flinke dosis oordeelsvorming van het bestuur. De meeste schattingen zijn gebaseerd op voorspellingen van hoe zaken zich in de toekomst zullen ontwikkelen. Sommige schattingen zijn relatief routinematig, andere zijn (zeer) complex door een groot aantal aannames, zoals pensioenverplichtingen. Daarbij kunnen kleine

veranderingen in elke aanname grote gevolgen hebben voor het geschatte bedrag. (Sensitieve) schattingen zijn subjectief en onzeker en brengen risico’s met zich mee voor de rapportage. De auditcommissie stelt zichzelf dus op de hoogte van belangrijke schattingen, welke veronderstellingen daaraan ten grondslag liggen en welk effect ze kunnen hebben op de resultaten (een sensitiviteits- of scenarioanalyse kan hierbij helpen).

Meest voorkomende schattingen

- oninbare vorderingen;
- oude of overtollige voorraden;
- waardering van (immateriële vaste) activa;
- pensioenverplichtingen en andere verplichtingen aan oud-medewerkers
- latente belastingvorderingen en schulden;
- waardering van financiële instrumenten (bijvoorbeeld leningen, aandelen, obligaties en derivaten);
- garantie-aanspraken;
- voorzieningen voor geschillen, lopende rechtszaken en claims;
- milieucclaims en kosten voor klimaatbeleid;
- reorganisatiekosten.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen

8. Crisis

9. Communicatie

Bandbreedte bij schattingen: voorzichtig tot agressief

Het bestuur hanteert bij schattingen verschillende bandbreedtes, waarbij de schatting kan variëren van voorzichtig tot agressief. Dat bepaalt uiteindelijk welk bedrag er in de boeken terecht komt. Tijdens de verslagperiode kunnen de aannames veranderen waarop de schattingen zijn gebaseerd. Ook de inschatting van het bestuur kan veranderen van conservatief/voorzichtig naar agressief of omgekeerd. Het bestuur stelt de auditcommissie daarvan op de hoogte en schetst de gevolgen: welk effect heeft dat op de resultaten en (bij beursgenoteerde bedrijven) op de winst per aandeel?

Hoe betrouwbaar zijn schattingen?

Een effectieve auditcommissie is alert op de redelijkheid en betrouwbaarheid van schattingen en gaat de discussie aan over de manier waarop het bestuur schattingen benadert, de aannames waarop deze zijn gebaseerd, de sensitiviteit daarvan voor de hoogte van de schatting. Voor de schatting en de resultaten en het trackrecord van het bestuur: hoe vaak klopten de schattingen en wanneer zat het bestuur ernaast?

Buitengewone of incidentele baten en lasten

De verkoop van een dochteronderneming, schade aan een productiefaciliteit door een grote brand, of een hoge boete van de externe toezichthouder: het zijn voorbeelden van eenmalige gebeurtenissen, transacties of verplichtingen die leiden tot bijzondere inkomsten of kosten en

die het (kwartaal-) resultaat aanzienlijk kunnen beïnvloeden. Organisaties kiezen er soms voor om deze buitengewone of incidentele baten en lasten niet als onderdeel van het operationeel resultaat te communiceren naar aandeelhouders, analisten en andere stakeholders. Beursanalisten en externe toezichthouders staan daar soms gereserveerd tegenover. Enerzijds zorgt het communiceren van buitengewone of incidentele baten en lasten

ervoor dat de reguliere operationele prestaties goed van periode tot periode vergeleken kunnen worden. Dit helpt beursanalisten bij hun aandelenadviezen. Anderzijds is het van belang kritisch te beoordelen of de werkelijke prestaties van de organisatie niet vertekend worden en of de organisatie inconsistent omgaat met incidentele resultaten in verschillende verslagperiodes: alleen erover communiceren wanneer het een positief

effect heeft op de resultaten en niet andersom. De huidige verslaggevingsstandaarden bieden weinig ruimte voor het classificeren van baten en lasten als buitengewoon of incidenteel. Wees daarom als auditcommissie alert op dit punt.

Wees alert op misleiding en let op consistentie

Een effectieve auditcommissie besteedt tijd en aandacht aan baten en lasten die als incidenteel, niet-regulier of buitengewoon gepresenteerd worden, heeft zicht op de omvang en het effect ervan op de resultaten en houdt adequaat toezicht op een juiste boekhoudkundige verwerking en rapportage. Is de verklaring van het bestuur om deze baten en lasten apart te communiceren redelijk en past de aangegeven invloed ervan op het resultaat bij het beeld dat de auditcommissie van de organisatie heeft? Sluit de externe rapportage op dit punt ook aan op de interne managementrapportage? Het belangrijkste is dat de auditcommissie zich ervan verzekerd heeft dat de rapportage over incidentele of buitengewone baten en lasten niet misleidend is en dat de communicatie van de organisatie erover consistent is in de verschillende verslagperiodes en via alle ingezette communicatiekanalen.

Inschatten of schattingen redelijk zijn

- Inventariseer welke rapportages belangrijke schattingen bevatten. Tip: het accountantsverslag bevat een overzicht van de belangrijkste schattingen. Ook worden in de niet-standaardpassages in de bevestiging bij de jaarrekening van het bestuur voor de externe accountant vaak de posten genoemd waarbij het eigen oordeel van het bestuur of het management een grote rol heeft gespeeld.
- Ga met het bestuur de discussie aan over de betrouwbaarheid van het proces, de systemen en de gegevens die ten grondslag liggen aan schattingen.
- Ga na hoe schattingen zich in het verleden verhielden tot de werkelijke resultaten.
- Doorgrond de belangrijkste aannames en afhankelijkheden waarop schattingen zijn gebaseerd en of deze zijn veranderd, of zouden moeten veranderen.
- Check de mate waarin het bestuur gebruikmaakt van modellen voor het doen van complexe schattingen – zoals pensioenverplichtingen of de waardering van derivaten – en hoe valide deze zijn (bijvoorbeeld door deze te laten testen door derden).
- Overweeg hoe groot de kans is dat de gebeurtenissen waarop de schattingen zijn gebaseerd ook daadwerkelijk zullen plaatsvinden.
- Doorgrond de redenen voor de timing en de bedragen van reserveringen, zoals het treffen van reorganisatievoorzieningen en het herzien van waarderingen van activa.
- Begrijp hoe een kleine verandering in de aanname voor een schatting het geactiveerde bedrag kan beïnvloeden, bijvoorbeeld met behulp van een sensitiviteits- of scenarioanalyse die het bestuur heeft voorbereid.
- Betrek de externe accountant of een derde partij bij het toetsen van de aannames of de gebruikte modellen.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekeningBijlagen
- 8. Crisis
- 9. Communicatie

Best practice

Beoordeel als auditcommissie of **non recurring**, 'eenmalige' of 'incidentele' resultaten ook daadwerkelijk incidenteel of eenmalig zijn. Of zijn er bijvoorbeeld elke periode wel afboekingen op de voorraad of reorganisatiekosten?

Zicht op buitengewone of incidentele baten en lasten

- Zorg dat het bestuur een eenduidige definitie hanteert van buitengewone of incidentele baten en lasten en dat deze consistent wordt toegepast.
- Wees alert op de positieve of negatieve invloed van buitengewone of incidentele baten en lasten op de resultaten in de verslagperiode.
- Check of het bestuur van plan is om de invloed van de buitengewone of incidentele baten en lasten op het resultaat apart te rapporteren.
- Controleer of het bestuur consistent omgaat met buitengewone of incidentele baten en lasten in verschillende verslagperiodes.
- Vraag of de organisatie consistent communiceert over buitengewone of incidentele baten en lasten via alle kanalen: op de website, in persberichten, tijdens contacten met aandeelhouders en in analistenrapporten.
- Vraag of het bestuur kan voorzien in alternatieve prestatie-indicatoren waarmee stakeholders de resultaten van de organisatie kunnen beoordelen.



2. Beoordelen van het bestuursverslag

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekeningBijlagen
- 8. Crisis
- 9. Communicatie

Toezicht houden op het bestuursverslag

Onderdeel van het jaarverslag is het bestuursverslag. Enerzijds dien het bestuursverslag te voldaan aan de van toepassing zijnde wet- en regelgeving (zie bijlage 7B op pagina xx), anderzijds kan de organisatie het bestuursverslag gebruiken om op vrijwillige basis financiële en niet-financiële informatie te delen. Stakeholders hechten een groter belang aan een informatief bestuursverslag. Europese regelgeving verlangt dat steeds meer niet-financiële informatie – vaak gelieerd aan duurzaamheid – wordt toegelicht in het bestuursverslag: hoe legt het bestuur daarover verantwoording af? Denk hierbij aan de informatie voortvloeiend uit de EU Taxonomy for sustainable activities en de Corporate Sustainability Reporting Directive (CSRD).

Best practice

Het instellen van een disclosure committee kan de auditcommissie helpen bij een goede invulling van haar toezichtrol. Een disclosure committee is verantwoordelijk voor de monitoring van de juistheid en volledigheid van de informatie in de toelichtingen op de jaarrekening en het bestuursverslag en rapporteert hierover aan zowel het bestuur als de auditcommissie.

¹ Voor het bestuursverslag worden ook wel termen gehanteerd als directieverslag, managementrapportage en jaarverslag (artikel 397 BW2)

De EU Taxonomie voor duurzame activiteiten

De EU Taxonomie voor duurzame activiteiten is een classificatiesysteem dat voor de belangrijkste activiteiten van de organisatie beschrijft wanneer deze als ‘duurzaam’ mogen worden bestempeld. De EU heeft zes milieudoelstellingen uitgewerkt:

- mitigeren van klimaatverandering
- aanpassing aan de klimaatverandering
- bescherming van water en maritieme hulpbronnen
- transitie naar een circulaire economie
- preventie van vervuiling
- bescherming van biodiversiteit en ecosystemen)

alsmede sociale en governance doelstellingen.

Ondernemingen moeten eerst vaststellen welke activiteiten beschreven zijn in de EU Taxonomy (**eligibility**) en in hoeverre deze aan de normen voldoen om duurzaam genoemd te mogen worden (**alignment**).

Voor financiële instellingen gelden andere en aanvullende regels.



De Corporate Sustainability Reporting Directive (CSRD)

De CSRD heeft vier pijlers:

1. verbreding van de toepassingsscope naar grote ondernemingen;
2. gedetailleerde rapportageverplichtingen waarbij ook de keten en het dubbele materialiteitsprincipe (zie hoofdstuk 3) moet worden meegenomen;
3. publicatie in het bestuursverslag, met toenemende verantwoordelijkheden voor governance organen;
4. verplichte externe verificatie met een beperkte mate van zekerheid.

Inhoudelijk moeten de volgende Europese Sustainability Reporting Standards (ESRS) worden verwerkt:

- korte beschrijving van het bedrijfsmodel en de strategie, inclusief haar veerkracht;
- doelstellingen met betrekking tot duurzaamheidskwesties die door het bedrijf zijn vastgesteld en de geboekte vooruitgang bij het bereiken van die doelstellingen;
- rol administratieve, bestuurlijke en toezichthoudende organen;
- beleid met betrekking tot duurzaamheidskwesties;
- voornaamste risico's en afhankelijkheden en het managen van die risico's;
- indicatoren die relevant zijn voor de openbaarmaking van informatie waarnaar wordt verwezen in de punten 1 tot en met 5 hierboven, en de openbaarmakingen van de EU Taxonomie voor duurzame activiteiten;
- immateriële activa: intellectueel, menselijk, sociaal en relationeel kapitaal;
- proces uitgevoerd om de informatie opgenomen in het bestuursverslag te identificeren en rekening te houden met korte, middellange en lange termijn horizon;
- due diligence-proces en de belangrijkste nadelige gevolgen voor het bedrijf en zijn waardeketen.



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekeningBijlagen
- 8. Crisis
- 9. Communicatie

Beoordelen van het bestuursverslag

- Voorziet het bestuursverslag in echte duiding en analyse, zodat stakeholders in staat worden gesteld om de organisatie te zien door de ogen van het bestuur en de belangrijkste financiële en niet-financiële indicatoren te gebruiken die het bestuur hanteert?
- Verrijkt de rapportage de (niet-)financiële verslaggeving en schetst deze een relevante context voor de analyse van de financiële situatie waarin de organisatie zich bevindt?
- Bevat de rapportage informatie over de kwaliteit van en mogelijke veranderingen in de resultaten en cashflow, zodat aandeelhouders kunnen bepalen hoe waarschijnlijk het is dat de gerapporteerde resultaten een indicatie vormen voor de resultaten in de toekomst?
- Is de rapportage helder en transparant en in begrijpelijke taal geschreven?
- Is voor de belangrijkste informatie de meest prominente plek ingeruimd?
- Worden in de rapportage belangrijke gebeurtenissen, trends en onzekerheden besproken, die aangeven dat prestaties in het verleden niet noodzakelijkerwijs een indicatie vormen voor toekomstige resultaten, bijvoorbeeld zaken die in de komende perioden tot aanpassingen zouden kunnen leiden?
- Beschrijft de rapportage het vermogen van de organisatie om in de financieringsbehoefte voor zowel de korte als de lange termijn te voorzien?
- Is de rapportage consistent en vergelijkbaar met die in eerdere verslagperioden en met resultaten in het verleden, sectornormen en de verwachtingen van stakeholders?
- Biedt de rapportage aanvullende inzichten, in plaats van alleen het herhalen van de voetnoten bij de jaarrekening?
- Worden in de rapportage de verslaggevingsregels niet alleen naar de letter, maar ook naar de geest nageleefd, door niet alleen te rapporteren over de vorm, maar ook over de inhoud van belangrijke gebeurtenissen, transacties en bijvoorbeeld de governance? Dit is van toepassing voor financiële en niet-financiële informatie.
- Biedt de rapportage een vooruitblik of toekomstperspectief: verwachte trends in business, markt, sector, concurrentieveld, et cetera?
- Hoe weet het bestuur dat in het bestuursverslag alle toelichtingen zijn opgenomen conform de geldende voorschriften voor het bestuursverslag (uit hoofde van BW2, Richtlijnen voor de jaarverslaggeving, EU-richtlijnen, Besluit inhoud bestuursverslag, governancecodes, et cetera)?

Voor een overzicht van de vereisten vanuit wet- en regelgeving voor het bestuursverslag wordt verwezen naar bijlage 7B.

De rol van de auditcommissie

De verantwoordelijkheid van de auditcommissie voor het bestuursverslag is tweeledig. De auditcommissie bekijkt of de informatie juist is, maar ook of deze volledig is. (Zie ook bijlage 7B.) Een effectieve auditcommissie gaat de discussie met het bestuur aan over dit soort zaken. Bijvoorbeeld wanneer het bestuur bepaalde informatie niet publiceert, omdat deze concurrentiegevoelig zou zijn, of de organisatie in verlegenheid zou kunnen brengen. Dat laatste zou voor de auditcommissie geen geldige reden mogen zijn om in te stemmen met het niet publiceren. Zo dient een auditcommissie specifieke aandacht te hebben voor duurzaamheidsinformatie in het bestuursverslag. Besturen hebben de neiging om

positieve duurzaamheidsprestaties uitgebreider toe te lichten dan de negatieve impact op van de onderneming (met het risico op **greenwashing**). Ook worstelen organisaties vaak met het bepalen van hoe ver zij in de keten moeten rapporteren. Met Europese wetgeving heeft de auditcommissie hier een rol te spelen.

Transparant over risico's

De auditcommissie ziet erop toe dat de organisatie open en eerlijk is over de robuustheid van het risicomanagement, de tekortkomingen daarin en de belangrijkste risico's, zowel in de risicoparagraaf als in de verklaring omtrent risicobeheersing (VOR) van het bestuur.. De auditcommissie kan daarbij haar andere toezichtstaak betrekken: de monitoring van de

Vragen die de auditcommissie kan stellen over duurzaamheidsrapportage

- Welke aanvullende mensen en middelen zijn mogelijk nodig om nieuwe duurzaamheidsinformatie- processen te implementeren en te beheersen?
- Hoe weet het bestuur dat alle wettelijke voorgeschreven toelichtingen zijn opgenomen in het bestuursverslag?
- Hoe verzamelt het bedrijf duurzaamheidsinformatie? Wat is het beleid voor deze informatieverzameling?
- Welke interne beheersing is er om ervoor te zorgen dat duurzaamheidsinformatie betrouwbaar en volledig is?
- Wat is de betrokkenheid van Internal Audit? Wat zijn hun bevindingen en aanbevelingen?
- Wat is de rol van de **disclosure commissie** in het hele proces?
- Wordt het hele verhaal verteld? Weerspiegelen de geschetste resultaten de werkelijke gang van zaken, of wordt de situatie vertekend weergegeven?
- Is de informatie in het bestuursverslag in lijn met de jaarrekening en de interim-rapportages?

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen
8. Crisis
9. Communicatie

Best practice		
Material methodologies, assumptions and definitions applied The basis for preparation, including the material methodologies and assumptions applied in the preparation of this consolidated sustainability statement, are included at the relevant disclosures to the consolidated sustainability statement. This includes specific reporting definitions as presented on pages 379 to 382 in the Glossary and definitions appendix. These methodologies, assumptions and definitions have been consistently applied across the years presented, and consistently during the financial year under review, unless stated otherwise.	sustainability statement in this Annual Report. This means that the company ensures that the information this report provides is: • Accurate: Precise and with sufficient level of detail • Balanced: Reflects relevant, and both positive and negative, aspects of performance • Clear: Understandable and accessible for stakeholders • Comparable: Consistent and allows for comparability over time • Complete: Sufficient to assess impacts during the reporting period • Sustainable context: About impacts of sustainable development • Timely: Allow stakeholders to make informed decisions • Verifiable: Auditable.	We aim to report based on actual data wherever possible. In some cases, we apply extrapolation to determine the performance of smaller entities, provided this yields reasonably predictable results. Further insights into the use of extrapolations can be found on page 378 in the Data extrapolation table in the Appendices. To ensure consistent and reliable reporting, PostNL has established company-wide definitions for each KPI and ESRS data point. Additionally, we have implemented formal quality controls within our reporting system. Both data owners (first line) and the control department (second line) conduct decentralised and centralised analyses to assess accuracy, completeness, and explain unexpected trends. These controls form part of an integrated internal control framework, covering both financial and sustainability reporting.
Note that the numbers presented in the sustainability statement and disclosures thereto may not sum precisely to the totals provided, and percentages may not precisely reflect the absolute figures due to rounding.	Processes, systems and controls PostNL employs structured and formalised processes to record, validate, and consolidate sustainability data for both key performance indicators (KPIs) and ESRS data points. ESG-related KPIs are integrated into the regular planning and control cycle, including budgeting, target setting, and periodic performance monitoring. We collect and report sustainability performance data on selected KPIs monthly, while other indicators are reported biannually or annually, depending on their nature.	However, the internal control framework for sustainability data is still maturing and not yet as advanced as that for financial reporting. This is due to inherent limitations, such as the evolving regulatory landscape, diverse data sources, manual processes, and limited automated controls. Over the coming years, we will take further steps to strengthen this framework.
Integrated reporting as guidance The Integrated Reporting framework of the International Integrated Reporting Council (IIRC) provides guidance on how companies should communicate about value creation. PostNL used the guiding principles and main content elements of the framework as input for this Annual Report. PostNL aims to further develop its corporate reporting communication on long-term value creation.	Each reporting entity is responsible for managing its sustainability data and actively monitoring its performance. While most data is recorded in central PostNL systems, additional systems are used for certain entities and indicators. To ensure a seamless consolidation process, we use an integrated IT system that captures both financial and sustainability data. Certain indicators, such as employee engagement, are collected and processed centrally.	Disclosures in relation to specific circumstances To provide an understanding of the effect of specific circumstances on the preparation of the sustainability statement, we disclose upon these if applicable.
Quality principles In line with the qualitative characteristics of information, PostNL applied high quality standards when preparing the		Time horizons We define the time horizons for reporting purposes in line with ESRS 1, respectively: • Short term: one year or less, 2025 • Medium term: two to five years, 2026 - 2030 • Long term: over five years, 2031 and later.
Bron: <u>Jaarverslag Post NL 2024</u>		

effectiviteit van de interne risicobeheersings- en controlesystemen en het analyseren en bespreken van materiële risico's en onzekerheden. Hierbij moet ook rekening gehouden worden met risico's vanuit duurzaamheidsaspecten, waaronder klimaatverandering. Vaak heeft een onderneming niet alleen impact op klimaatverandering, maar heeft klimaatverandering ook impact op de onderneming in de vorm van risico's en kansen. Van daaruit kan de auditcommissie de integriteit en kwaliteit van de risicoparagraaf en de bestuursverklaring beoordelen: communiceert het bestuur juist, volledig en waarheidsgetrouw over de risico's waarmee de organisatie wordt geconfronteerd en hoe wordt daarmee omgegaan?

In de Corporate Governance Code 2025 is de onderbouwing voor de verantwoording over risicobeheersing uitgewerkt, zie pagina 63 (verwijzing naar VOR in deze publicatie, check of deze nummering klopt)

De code geeft aan hoe het bestuur verantwoording aflegt over de effectiviteit van de opzet en werking van interne risicobeheersings- en controlesystemen. Het bestuur bespreekt dit met de auditcommissie en legt daarover verantwoording af aan de raad van commissarissen. Deze verantwoording wordt in het bestuursverslag opgenomen als onderdeel van het jaarverslag openbaar gemaakt.

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen

8. Crisis

9. Communicatie

Best practice

Internal controls over sustainability reporting

Besi's internal control and risk management function operates under the responsibility of the Board of Management and is monitored on an ongoing basis. The Supervisory Board oversees the internal control and risk management function and maintains regular contact with the persons fulfilling this function. Besi's internal control system consists of a formal framework defining key risks and key controls over financial reporting, an internal control charter outlining audit systems and procedures as well as the internal control and audit plan for the year. Operational, IT, compliance, tax and fraud controls are included in this framework. The internal control system over financial reporting also contains clear accounting rules. It has been implemented in substantially all operations and material subsidiaries and supports common accounting and regular financial reporting in standard formats.

Besi's sustainability strategy is influenced by important global trends currently such as climate change, natural resource conservation, pollution and the circular economy as well as social topics such as diversity, human rights, working conditions and the recruitment of qualified technical personnel. In addition, Besi's sustainability and non-financial risks are governed by a set of policies and procedures including ISO 14001 environmental management certification, Code of Conduct, Sustainability policy, Climate Transition Plan and Human Rights policy.

Our internal control and risk management systems are designed to address, identify and limit sustainability-related risk factors and non-financial risks that could affect both our strategy and business operations. Besi's sustainability reporting framework has been created to ensure that sustainability-related data is collected from our operations on a quarterly basis. Besi's sustainability team manages data collection, validation, aggregation and reporting to the Board of Management and Management Team consistent with its internal control framework. Internal controls for sustainability reporting vary based on the metrics being measured as multiple business units across Besi's geographies contribute to sustainability data collection. For instance, the definition of adequate wages may differ from country to country. At a consolidated level, control measures are in place to ensure accurate and complete reporting of sustainability-related metrics as part of our Annual Report. Any issues identified by the internal control framework are reported to the Board of Management.

We implement dedicated controls through our internal control system to ensure the development of a reporting framework based on our material impacts, risks and opportunities. To date, we have implemented the following internal controls:

- Gap assessment to identify policy-, procedure- and data gaps to meet CSRD requirements.
- Review of the 2024 sustainability reporting framework and its ability to meet CSRD requirements.
- Quarterly sustainability data collection, review and aggregation.

Bron: **Jaarverslag Besi 2024**

The sustainability-related risks are incorporated into our overall risk management approach. Besi's risk management program seeks to identify and control potential risks and events which may affect our strategy, continuity, business and performance. Mitigation strategies for sustainability-related risks include (i) the collection and analysis of sustainability-related KPIs, (ii) capital allocation towards projects which help mitigate identified risks, (iii) action plans with short-, medium- and long-term actions and targets and (iv) company-wide policies which are communicated throughout our value chains.

Sustainability-related risks can be identified through:

- Quarterly sustainability data collection, aggregation and discussion with the Management Team and the Board of Management.
- Internal control framework oversight of sustainability data collection and reporting.
- Engagement with Besi's stakeholders.
- Communication channels such as the Whistleblower procedure and Grievance procedure available for our own workforce, workers in the value chain and other stakeholders.
- Climate risk assessment.
- Double Materiality Assessment of sustainability-related impacts, risks and opportunities.

The Management Team is responsible for the monitoring and reporting of all identified risks as well as for leading the response across the organization with respect to any new risks which may arise. All material findings that result from the use of Besi's internal control and risk management system for financial and non-financial risks are discussed with the Board of Management on a monthly basis and with the Audit Committee as part of the Supervisory Board's review on a quarterly or semi-annual basis.

Besi's Annual Report shall include a report of the Supervisory Board in which it shall render an account of the supervision conducted for the previous financial year. The supervision of the Board of Management by the Supervisory Board shall include its responsibility relative to Besi's corporate strategy, the risks inherent in its business activities and the effectiveness of the design and operation of its internal risk management and control systems. The report shall also include an account of the Supervisory Board's involvement in the establishment of a sustainable long-term value creation strategy and the way in which it monitors its implementation.

In addition to internal controls over financial reporting, the external auditor reviews the process carried out by Besi to identify the information reported pursuant to the ESRS. The results of this audit are discussed with the Board of Management and the Audit Committee of the Supervisory Board.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen

8. Crisis

9. Communicatie

Het bestuur kan de continuïteitsveronderstelling bijvoorbeeld onderbouwen met een gedegen cashflowprognose voor de komende twaalf maanden. (Zie ook hoofdstuk 2: Continuïteit – langetermijnwaardecreatie.) Daarnaast kan de auditcommissie Internal Audit vragen een beoordeling hiervan te maken. (Zie verder hoofdstuk 4 voor een uitgebreide bespreking van de rol van de auditcommissie ten aanzien van risicobeheersing en interne controle/ verslaggevingsrisico’s en hoofdstuk 9 voor de communicatie daarover met het bestuur en de stakeholders.)

Beoordelen niet-financiële informatie en duurzaamheidsinformatie

Steeds meer organisaties komen tegemoet aan de roep van stakeholders om in het jaarverslag verantwoording af te leggen over hun sociaalmaatschappelijke opstelling. Daarnaast zijn Europese OOB’s met meer dan 500 werknemers verplicht om niet-financiële informatie te publiceren over de manier waarop zij omgaan met het milieu, sociale aspecten en personeelsaangelegenheden, mensenrechten, corruptie en omkoping, vertaald naar risico’s, kpi’s en resultaten. In de wet wordt dit geduid als ‘de verklaring niet-financiële informatie’. Ook wordt de druk steeds groter om te rapporteren over de gevolgen van klimaatverandering op het businessmodel. Zo roepen grote investeerders en belangenverenigingen zoals Eumedion op tot meer transparantie over hoe klimaatverandering impact heeft op de financiële ontwikkeling van de onderneming. Veel organisaties kiezen tegenwoordig voor geïntegreerde verslaggeving (financiële en

niet-financiële informatie in één jaarverslag). Zie ook hoofdstuk 3: Corporate impact.

Corporate-governanceverklaring

Beursgenoteerde ondernemingen moeten in een corporate-governanceverklaring rapporteren over onder andere de naleving van de Nederlandse Corporate Governance Code, eventuele andere gedragscodes en hun governancepraktijken in het algemeen. Daarbij wordt ook gerapporteerd over:

- Toezicht op het beleid van het bestuur en de algemene gang van zaken
- Samenstelling en functioneren van de RvC
- Verslag van de commissies binnen de RvC, zoals auditcommissie, remuneratiecommissie of selectie- en benoemingscommissie,
- Onafhankelijkheid van de commissarissen
- Beleid voor diversiteit en inclusie en de uitvoering daarvan.
- Integriteit en kwaliteit van de duurzaamheidsverslaggeving

In de laatste Corporate Governance Code van maart 2025 is de Verklaring omtrent Risicobeheersing toegevoegd. De RvC moet in haar verslag aandacht besteden aan de wijze waarop de effectiviteit van de opzet en werking van de interne risicobeheersings- en controlssystemen is beoordeeld, zie pagina 63.

Niet-financiële informatie laten toetsen door de externe accountant?

Bij de keuze van externe assurance voor niet-financiële informatie staat de auditcommissie voor de volgende afwegingen:

- toetsing op kwaliteit en integriteit;
- extra zekerheid ten aanzien van naleving;
- een accountant die vanuit een breder perspectief de onderneming in ogenschouw neemt;
- belang van assurance bij niet-financiële informatie in benchmarks door onafhankelijke partijen;
- praktijken binnen de sector en/of belangrijke peers;
- meer geloofwaardigheid naar stakeholders door externe en onafhankelijke controle, maar ook:
- additionele kosten voor de controle.

De rol van de auditcommissie

Een effectieve auditcommissie zal ook de niet-financiële verslaglegging zorgvuldig monitoren op kwaliteit en integriteit. De auditcommissie kan hierbij het perspectief hanteren van het compliance- en reputatierisico, als de organisatie niet of onvoldoende tegemoetkomt aan de Nederlandse en Europese regelgeving en aan maatschappelijke verwachtingen. Het rapporteren (en daarmee monitoren) van niet-financiële informatie kan een uitdaging vormen, omdat prestaties op dit gebied soms lastig te meten en te vergelijken zijn.

Kiezen voor externe ‘assurance’ bij niet-financiële informatie?

Een vraag voor de auditcommissie is of ook de niet-financiële informatie gecontroleerd moet worden door de externe accountant. Is het gewenst of noodzakelijk om bijvoorbeeld CO₂-emissies of andere duurzaamheidsverslaggeving,

medewerkersbetrokkenheid, klanttevredenheids- en cultuuraudits of opleidingsbudgetten te onderwerpen aan een apart onderzoek van Internal Audit of de externe accountant voor aanvullende **assurance**?

Vaak kiezen organisaties voor een beperkte mate van zekerheid van hun externe accountant bij deze informatie. Deze is verplicht voor ondernemingen die onder de CSRD vallen.

Mandaat verstrekken tijdens opdracht

Als de auditcommissie ook de niet-financiële informatie wil laten controleren, dan heeft het de voorkeur dat dit al wordt besproken tijdens de selectieprocedure van de externe accountant en meegenomen wordt in de opdrachtverstrekking. De auditcommissie kan de monitoring van niet-financiële informatie ook laten opnemen in het werkplan van Internal Audit. Zie ook hoofdstuk 6 voor de relatie van de auditcommissie met Internal Audit en de externe accountant.

3. Beoordelen van de financiële informatie buiten de jaarrekening

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekeningBijlagen
- 8. Crisis
- 9. Communicatie

Naast de jaarrekening publiceren organisaties soms ook op andere momenten in het jaar financiële informatie, zoals halfjaar- en kwartaalberichten. De bekendmaking van tussentijdse resultaten kan invloed hebben op de beurskoers, als deze niet voldoen aan de verwachtingen van beleggers of andere stakeholders, of deze juist overstijgen. De auditcommissie kan de discussie met het bestuur aangaan of de publicatie van bijvoorbeeld kwartaalresultaten wel gewenst is: het kan leiden tot een kortetermijnnoriëntatie, terwijl organisaties juist moeten streven naar duurzame langetermijnwaardecreeatie.

■ De rol van de auditcommissie

Toezicht houden op tussentijdse financiële informatievoorziening

Het is de verantwoordelijkheid van de auditcommissie om ook toezicht te houden op andere vormen van publieke rapportering die financiële informatie bevatten. In toenemende mate komt hier ook niet-financiële informatie in naar voren. Als er per kwartaal wordt gerapporteerd, doet de auditcommissie er verstandig aan intensief en proactief aandacht te besteden aan de tussentijdse resultaten, voordat deze worden gepubliceerd. In feite stelt de auditcommissie dezelfde vragen als bij de jaarrekening. De auditcommissie zal – voordat de resultaten en het bijbehorende persbericht worden gepubliceerd – onder meer het volgende willen weten:

- Is de opstelling van de interim-rapportages consistent met de jaarrekening?

- Is de interne beheersing van de totstandkoming van de financiële informatie op orde?
- Heeft de totstandkoming van de rapportages voldoende aandacht binnen de organisatie (is er sprake van eigenaarschap en betrokkenheid van het bestuur)?
- Is er sprake van lastige verslaggevingsissues?
- Welke rol heeft oordeelsvorming gespeeld?
- Hoe verhouden de resultaten zich tot het budget en de verwachtingen?
- Is er sprake van een positieve of negatieve trend?
- Hoe is omgegaan met bijvoorbeeld schattingen en incidentele of buitengewone baten en lasten?
- Hoe worden de resultaten gecommuniceerd?

De auditcommissie bespreekt ook de resultaten van de controle of de beoordeling van interim-rapportages door de externe accountant, indien deze daartoe opdracht heeft gekregen als onderdeel van de jaarrekeningcontrole, in de vorm van een zogenoemde reviewopdracht of specifiek overeengekomen werkzaamheden. De externe accountant zal in dat geval – net als bij de jaarrekening – de auditcommissie op de hoogte stellen van specifieke zaken in de controle of beoordeling, zoals een nieuwe of veranderde boekhoudkundige grondslag, voorgestelde aanpassingen en gevonden onregelmatigheden in de rapportage, verschil van mening met het bestuur en wijzigingen in de interne risicobeheersings- en controlesystemen. Het verdient aanbeveling dat de auditcommissie, in overleg met het bestuur, afspraken maakt met de

accountant over de wijze waarop deze betrokken wordt bij persberichten over de interim-resultaten en dit schriftelijk vast te leggen in de opdrachtbrief voor de externe accountant.

Bewaken ‘forward-looking statements’

Het bestuur blikt, naast de verplichte vooruitblik in het bestuursverslag, ook in persberichten en via andere communicatiekanalen soms vooruit naar de resultaten in de komende periode(n), zoals de verwachte ontwikkeling van de omzet, cashflow en winst per aandeel. Het vooruitlopen op toekomstige resultaten draagt bij aan een langetermijnnoriëntatie – zeker bij de publicatie van interim-resultaten. Aan de andere kant is voorspellen moeilijk: het vraagt veel eigen oordeelsvorming en schattingen van het bestuur. Dat brengt het risico met zich mee dat een forward-looking statement later moet worden aangepast. Bovendien brengt vooruitblikken naar toekomstige financiële en niet-financiële resultaten risico’s met zich mee op juridisch, concurrentie- en reputatiegebied. Het kan ook fungeren als een perverse prikkel voor het bestuur om de zelf gecreëerde verwachtingen te willen waarmaken. De auditcommissie zou met die mogelijkheid rekening moeten houden bij het beoordelen van de integriteit van de verslaggeving in de bewuste perioden en het beoordelen van de inhoud van de presentaties voor beleggers en analisten.

Protocol voor persberichten

Ook informatie waarin het bestuur duiding geeft aan de jaarcijfers en interim-resultaten – zoals persberichten en presentaties voor analisten, institutionele beleggers en ratingbureaus – verdient aandacht van de auditcommissie en de raad van commissarissen. Daarbij gaat het vooral om het samen met het bestuur ontwikkelen van protocollen voor de interne en externe communicatie van resultaten. De rol van de auditcommissie is erop toezien dat de informatie niet gekleurd of onevenwichtig is, maar in lijn is met de financiële en niet-financiële verslaggeving en een eerlijk en waarheidsgetrouw beeld geeft van de activiteiten en de positie van de organisatie in de verslagperiode.

Beleggers, analisten, ratingbureaus, kapitaalverstrekkers en toezichthouders baseren hun beslissingen mede op de vooruitblik van het bestuur naar verwachte resultaten. Gezien het grote belang dat daaraan wordt gehecht, zal de auditcommissie nauw betrokken willen zijn bij de beoordeling ervan. De auditcommissie bewaakt de kwaliteit en de integriteit van de informatie en let op de juridische consequenties en de risico’s op concurrentie- en reputatiegebied.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. **Corporate Reporting**
 1. Beoordelen van de financiële verslaggeving
 2. Beoordelen van het bestuursverslag
 3. Beoordelen van de financiële informatie buiten de jaarrekeningBijlagen
8. Crisis
9. Communicatie



Toezicht op de financiële vooruitblik

- Vraag het bestuur naar de filosofie achter het forward-looking statement: overweeg of het uitbrengen daarvan ondersteunend is aan langetermijnwaardecreatie en het remuneratiebeleid.
- Doorgrond de motivatie van het bestuur voor de financiële vooruitblik: is het een reactie op druk vanuit de kapitaalmarkt? Beoordeel of het bestuur de voor- en nadelen goed tegen elkaar heeft afgewogen.
- Verkrijg inzicht in het onderliggende proces: het formuleren van aannames/het doen van schattingen en het verzamelen van gegevens voor de uitgesproken verwachting. Zie erop toe dat het proces robuust is en dat de oordeelsvorming van het bestuur redelijk is.
- Beoordeel het protocol voor vooruitblikken en de richtlijnen voor het actualiseren daarvan bij kwartaalresultaten, voor zowel positieve als negatieve veranderingen.
- Houd het beleid regelmatig tegen het licht: past vooruitblikken nog bij opkomende trends, vigerende opinies in de markt en veranderende risico's?
- Benchmark aan sectorgenoten en concurrentie om de manier van vooruitblikken te beoordelen en in te schatten of de organisatie op dit gebied een buitenbeentje is.
- Wees alert op mogelijk **earningsmanagement** om aan de geschetste verwachtingen tegemoet te komen.

Bijlagen

Bijlage 7A	Vragen aan het bestuur bij de beoordeling van de jaarrekening
Bijlage 7B	Overzicht voorgeschreven toelichtingen in het bestuursverslag

Bijlage 7A Vragen aan het bestuur bij de beoordeling van de jaarrekening

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
 - 1. Beoordelen van de financiële verslaggeving
 - 2. Beoordelen van het bestuursverslag
 - 3. Beoordelen van de financiële informatie buiten de jaarrekening
- 8. Crisis
- 9. Communicatie

A. Proces van financiële verslaggeving

- Op welke terreinen bestaan momenteel de grootste financiële risico's en hoe worden deze beheerst?
- Beschikt de organisatie over de juiste administratieve systemen en zijn deze toereikend?
- Welke belangrijke aanbevelingen zijn (door de interne en/of externe accountant) aan het bestuur gedaan inzake verbeteringen van het verslaggevingsproces? Hoe heeft het bestuur gereageerd? Zijn er belangrijke gebieden die nog aandacht behoeven?
- Op basis van welke informatie heeft het bestuur zich ervan overtuigd dat de organisatie een **going concern** is (dat wil zeggen dat het in de nabije toekomst de activiteiten zal voortzetten)?
- Hoe beïnvloeden huidige geopolitieke ontwikkelingen en internationale handelsverhoudingen de financiële positie en de risico's van de organisatie? Welke maatregelen heeft het bestuur genomen om de hiermee gepaard gaande risico's te beheersen?

B. Grondslagen van waardering en resultaatbepaling

- Zijn de belangrijke grondslagen van waardering en resultaatbepaling nog steeds relevant? Zijn de hieraan ten grondslag liggende veronderstellingen nog steeds van toepassing?
- Zijn er dit jaar wijzigingen in de grondslagen van waardering en resultaatbepaling? Zo ja, wat zijn hiervoor de redenen en wat zijn de effecten van de wijzigingen?
- Welke effecten zou een eventueel nieuwe, algemeen aanvaarde grondslag van financiële ver-

slaggeving of andere richtlijn of een voorgestelde wijziging in een bestaande grondslag of richtlijn hebben op de jaarrekening?

- Was er sprake van verschil van mening tussen het bestuur en de accountant met betrekking tot de grondslagen van waardering en resultaatbepaling of de financiële verslaggeving? Is dit op bevredigende wijze opgelost?
- Hoe verhouden de grondslagen van de organisatie zich tot de norm binnen de bedrijfssector?
- Wat is de algemene indruk over de (on)voorzichtigheid van de gehanteerde grondslagen van waardering en resultaatbepaling en de gemaakte schattingen?
- Welke invloed hebben nieuwe technologieën en digitale transformatie op de waarderingsgrondslagen van de organisatie gehad? Zijn er specifieke technologische ontwikkelingen die de financiële verslaggeving of de operationele processen hebben veranderd?

C. Jaarrekening

- Wijkt de jaarrekening in belangrijke mate af van die van voorgaande jaren? Waardoor zijn deze afwijkingen veroorzaakt?
- Zijn er ongewone reserveringen/passiveringen in de balans opgenomen?
- Is er sprake geweest van correcties in verband met (een) voorgaande periode(n)? Wat was de achtergrond?
- Zijn er ongebruikelijke, tijdens het jaar afgewikkelde transacties geweest die niet uit de jaarrekening blijken? Hoe zijn deze transacties verantwoord? Zijn bij deze transactie(s) verbonden partijen betrokken geweest?

- Zijn er belangrijke zaken naar voren gebracht door het bestuur, de bedrijfsjurist of externe juridische adviseurs betreffende gerechtelijke procedures, onvoorziene gebeurtenissen, claims of belastingaanslagen? Hoe zijn dergelijke zaken in de jaarrekening verantwoord?
- Worden continuïteitskwesaties voldoende toegelicht? Bestaat het gevaar dat de organisatie niet voldoet aan voorwaarden van leningsovereenkomsten, niet-achtergestelde schulden en aandelenemissies?
- Hoe heeft het bestuur zich zekerheid verschafte over de waarde van langetermijnbeleggingen?
- Heeft de onderneming in 'exotische' financiële instrumenten belegd?
- Is de waarde van verhandelbare effecten of andere financiële instrumenten sinds het einde van het boekjaar belangrijk gewijzigd?
- Hoe verhoudt zich de gemiddelde ouderdom van debiteuren per het einde van het boekjaar tot het voorafgaande jaar?
- Hoe is de voorziening wegens dubieuze debiteuren bepaald? Bestaat er twijfel over de inbaarheid van grote individuele vorderingen?
- Zijn er belangrijke of ongebruikelijke bedragen te vorderen van functionarissen of werknemers? Zijn er andere belangrijke transacties met verbonden partijen?
- Welke stappen zijn ondernomen om de omvang van incurante of overtollige voorraden vast te stellen? Zijn er belangrijke afboekingen geweest?
- Zijn er plannen of programma's van de overheid of regelgevende en/of toezichthoudende instanties, bijvoorbeeld met betrekking tot het milieu, die de

waardering van posten negatief zouden kunnen beïnvloeden of die de vorming van een voorziening noodzakelijk maken?

- Hoeveel aandacht is geschonken aan mogelijke problemen als gevolg van onteigening van of beperkingen op het gebruik van activa?
- Welke jaren zijn fiscaal nog niet afgewikkeld? Zijn er belangrijke posten waarover (mogelijk) onenigheid bestaat?
- Zijn er (voorwaardelijke) verplichtingen die mogelijk aanleiding geven tot waardevermindering van een activum of vorming van een verplichting/schuld die niet in de jaarrekening is opgenomen?

D. Algemene vragen

- Zijn er problemen aan het ontstaan die dit jaar niet verwerkt of vermeld hoeven te worden, maar, indien de omstandigheden niet verbeteren, mogelijk wel volgend jaar aan de orde komen?
- Wat is uw grootste zorg ten aanzien van de financiële positie van de onderneming?

E. Uitvoering van de controle door de externe accountant

- Zijn er naar aanleiding van de controle belangrijke correcties in de jaarrekening aangebracht?
- Zijn er naar aanleiding van de controle niet-doorgevoerde correcties geweest?

Zie hoofdstuk 6, deel 2 (de relatie met de externe accountant) voor een uitgebreide bespreking van vragen die de auditcommissie kan stellen over de uitvoering van de controle door de externe accountant.

Bijlage 7B Overzicht voorgeschreven toelichtingen in het bestuursverslag

Overzicht toelichtingen (disclosures) op te nemen in bestuursverslag (gebaseerd op RJ-400 editie 2019)

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen
8. Crisis
9. Communicatie

Grondslag	Reikwijdte	Disclosure topic	Disclosure-element – korte omschrijving
A. Disclosures op basis van rechtsvorm [Artikel 2:391 BW2]	Alle grote en middelgrote organisaties	A1 Doelstelling en kernactiviteiten	Doelstelling / mission statement Kernactiviteiten
		A2 Structuur en personele bezetting	Juridische structuur Interne organisatiestructuur en personele bezetting
		A3 Beleid en verwachtingen	Belangrijke elementen van het gevoerde beleid en de gang van zaken Belangrijke aangelegenheden waarover in het voorgaande bestuursverslag verwachtingen werden uitgesproken dan wel een belangrijke onzekerheid werd vermeld.
		A4 Financiële ontwikkelingen	Ontwikkelingen gedurende het boekjaar Behaalde omzet en resultaten Toestand op balansdatum (solvabiliteit en liquiditeit) Kasstromen en financieringsbehoeften Verwijzingen naar en aanvullende uitleg over posten in de jaarrekening Financiële prestatie-indicatoren
		A5 Risico's en risicobeheersing	Voornaamste risico's en onzekerheden Risicobereidheid Maatregelen ter beheersing van de voornaamste risico's en onzekerheden Impact op resultaten en/of financiële positie indien risico's zich zouden voordoen Risico's en onzekerheden met belangrijkste impact in het afgelopen boekjaar Verbeteringen in het systeem van risicomanagement Wijze waarop het systeem van risicomanagement is verankerd in de organisatie
		A6 Cultuur & gedrag	Maatregelen ter beïnvloeding van de cultuur, het gedrag en de motivatie van werknemers (soft controls)
		A7 Risicobeheer financiële instrumenten	Doelstellingen en het beleid inzake risicobeheer van financiële instrumenten Beleid inzake de afdekking van risico's verbonden aan alle belangrijke soorten voorgenomen (financiële) transacties Gelopen prijs-, krediet-, liquiditeits- en kasstroomrisico's
		A8 Gedragscodes	Gedragscodes die gevolgd worden Verwijzing naar informatie over de naleving van gedragscodes
		A9 Onderzoek en ontwikkeling	Werkzaamheden op het gebied van onderzoek en ontwikkeling
		A10 Overige informatie	Onderwerpen die van belang kunnen zijn: - marketing en distributie - interne beheersing van processen en procedures - kwaliteitsbeheersing - informatievoorziening intern en extern, en - automatisering
		A11 Toekomstverwachtingen	Verwachte gang van zaken met betrekking tot: - investeringen - financiering - personeelsbezetting - omstandigheden waarvan de ontwikkeling van de omzet en de rentabiliteit afhankelijk is

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen
8. Crisis
9. Communicatie

Grondslag	Reikwijdte	Disclosure topic	Disclosure-element – korte omschrijving
D. Eventuele additionele disclosures op basis van beursgenoteerde effecten	Genoteerde (certificaten van) aandelen of andere effecten aan een gereglementeerde EER markt	D1 Bestuursverklaring financiële verslaggeving	Bestuursverklaring over getrouw beeld jaarrekening, getrouw beeld bestuursverslag en beschrijving voornaamste risico's
[Wet op het financieel toezicht]			
[Besluit inhoud bestuursverslag]	Genoteerde effecten niet zijnde aandelen op een gereglementeerde EER markt	D2a Corporate governance disclosures - verklaring inzake corporate governance	Belangrijkste kenmerken beheersings- en controlesysteem proces financiële verslaggeving
[Besluit artikel 10 Overnamerichtlijn]			Diversiteitsbeleid (doelstelling, uitvoering, resultaten) samenstelling bestuur en de raad van commissarissen [NB: mits grote onderneming]
[Nederlandse Corporate Governance Code]	Genoteerde (certificaten van) aandelen op een gereglementeerde EER markt of multilaterale handelsfaciliteit (MTF).	D2b Corporate governance disclosures - verklaring inzake corporate governance	- Naleving (en gemotiveerde afwijkingen) van de Nederlandse Corporate Governance Code en eventuele (vrijwillige) naleving andere gedragscodes en governance praktijken - Referentie aan waar de gehele tekst van de Nederlandse Corporate Governance Code beschikbaar is voor het publiek - Belangrijkste kenmerken beheers- en controlesysteem proces financiële verslaggeving - Functioneren van de algemene vergadering van aandeelhouders, haar bevoegdheden en rechten van aandeelhouders voor zover niet onmiddellijk volgend uit de wet - Samenstelling en functioneren van het bestuur en de raad van commissarissen en hun commissies - Diversiteitsbeleid (doelstelling, uitvoering, resultaten) samenstelling van bestuur en de raad van commissarissen [NB: mits grote onderneming] - Een aantal toelichtingen uit hoofde van artikel 10 Overnamerichtlijn: c,d, f, h, en i (zie verder D3), alsmede een disclosure volgend uit artikel 392 lid1 e: een opgave van het aantal stemrechtloze aandelen en het aantal aandelen dat geen of slechts een beperkt recht geeft tot deling in de winst of reserves van de vennootschap, met vermelding van de bevoegdheden die zij geven.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening

Bijlagen
8. Crisis
9. Communicatie

Grondslag	Reikwijdte	Disclosure topic	Disclosure-element – korte omschrijving
D. Eventuele additionele disclosures op basis van beursgenoteerde effecten	Genoteerde (certificaten van) aandelen aan een gereguleerde EER markt	D3 Governance disclosures artikel 10 Overnamerichtlijn	Disclosures uit hoofde van artikel 10 overnamerichtlijn (indien van toepassing): a. de kapitaalstructuur van de vennootschap, het bestaan van verschillende soorten aandelen en de daaraan verbonden rechten en plichten en het percentage van het geplaatste kapitaal dat door elke soort wordt vertegenwoordigd; b. elke beperking door de vennootschap van de overdracht van aandelen of met medewerking van de vennootschap uitgegeven certificaten van aandelen; c. deelnemingen in de vennootschap waarvoor een meldingsplicht bestaat overeenkomstig de artikelen 5:34, 5:35 en 5:43 van de Wet op het financieel toezicht; d. bijzondere zeggenschapsrechten verbonden aan aandelen en de naam van de gerechtigde; e. het mechanisme voor de controle van een regeling, die rechten toekent aan werknemers om aandelen in het kapitaal van de vennootschap of een dochtermaatschappij te nemen of te verkrijgen, wanneer de controle niet rechtstreeks door de werknemers wordt uitgeoefend; f. elke beperking van stemrecht, termijnen voor de uitoefening van stemrecht en de uitgifte, met medewerking van de vennootschap, van certificaten van aandelen; g. elke overeenkomst met een aandeelhouder, voor zover aan de vennootschap bekend, die aanleiding kan geven tot beperking van de overdracht van aandelen of met medewerking van de vennootschap uitgegeven certificaten van aandelen of tot beperking van het stemrecht; h. de voorschriften betreffende benoeming en ontslag van bestuurders en commissarissen en wijziging van de statuten; i. de bevoegdheden van het bestuur, in het bijzonder tot de uitgifte van aandelen van de vennootschap en de verkrijging van eigen aandelen door de vennootschap; j. belangrijke overeenkomsten waarbij de vennootschap partij is en die tot stand komen, worden gewijzigd of ontbonden onder de voorwaarde van een wijziging van zeggenschap over de vennootschap nadat een openbaar bod in de zin van artikel 5:70 van de Wet op het financieel toezicht is uitgebracht, evenals de gevolgen van die overeenkomsten, tenzij de overeenkomsten of gevolgen zodanig van aard zijn dat de vennootschap door de mededeling ernstig wordt geschaad; k. elke overeenkomst van de vennootschap met een bestuurder of werknemer die voorziet in een uitkering bij beëindiging van het dienstverband naar aanleiding van een openbaar bod in de zin van artikel 5:70 van de Wet op het financieel toezicht.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting

1. Beoordelen van de financiële verslaggeving

2. Beoordelen van het bestuursverslag

3. Beoordelen van de financiële informatie buiten de jaarrekening
- Bijlagen
8. Crisis
9. Communicatie

Grondslag	Reikwijdte	Disclosure topic	Disclosure-element – korte omschrijving
D. Eventuele additionele disclosures op basis van beursgenoteerde effecten	Nederlandse nv met genoteerde (certificaten van) aandelen op een gereguleerde markt of MTF	D4 Corporate governance disclosures uit hoofde van de Nederlandse Code Corporate Governance	- Hoofddlijnen corporate governance van de vennootschap - Gemotiveerde uitleg (wijze, redenen, tijdsduur, alternatieve maatregel) van afwijkingen (principes en best practices) van de Code; ‘pas toe of leg uit’ - Visie op langetermijnwaardecreatie en de strategie ter realisatie daarvan - Inbedding van waarden in de organisatie - Werking en naleving van de door het bestuur opgestelde gedragscode - Diversiteitsbeleid van de raad van commissarissen/raad van bestuur - Executive committee (indien van toepassing) disclosures: keuze, rol en taak en samenstelling, en de wijze van contact tussen de draad van commissarissen en de excutive committee - Transacties waarbij tegenstrijdige belangen van bestuurders of commissarissen spelen - Transacties met aandeelhouders die ten minste 10% van de aandelen houden - Overzicht beschermingsmaatregelen tegen een overname van zeggenschap - Verantwoording over risico's en risicomanagement: (a) risicobeoordeling en risicoprofiel in relatie tot de risicobereidheid; (b) opzet en werking interne risicobeheersings- en controlesystemen over het afgelopen boekjaar (c) eventuele belangrijke tekortkomingen, wijzigingen en verbeteringen in de interne risicobeheersings- en controlesystemen en bespreking ervan met de auditcommissie en de raad van commissarissen; (d) gevoeligheid van de resultaten voor materiële wijzigingen in externe omstandigheden. - Bestuursverklaring over risico's, tekortkomingen in interne risicobeheersing en controlesystemen, financiële verslaglegging op basis van continuïteitsveronderstelling en risico's in relatie tot continuïteit



Misstanden en onregelmatigheden – wat te doen?

08

8. Misstanden en onregelmatigheden – wat te doen?

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Het is niet de vraag óf maar wannéér een organisatie met een crisis wordt geconfronteerd. Misstanden en onregelmatigheden kunnen een belangrijke oorzaak vormen voor het ontstaan van een crisis. De auditcommissie speelt een cruciale rol bij het toezicht op het onderzoek naar fraude of andere integriteitsproblemen (of stuurt dat zelf aan) en op het herstelplan.

Misstanden en onregelmatigheden, zoals het ontduiken van wet- en regelgeving, integriteitsschendingen, belangenverstrengeling, (boekhoud)fraude of corruptie kunnen leiden tot een ernstige crisis, die de reputatie van de organisatie en zelfs de continuïteit kan bedreigen. Bij misstanden en onregelmatigheden kan het immers gaan om ontvreemding van grote geldbedragen of kostbare assets, hoge boetes en reputatieschade, mogelijk leidend tot een boycot, problemen in de keten of het verlies van de **licence to operate**. Een crisis vraagt om adequaat toezicht en zo nodig tijdig ingrijpen door de raad van commissarissen/de auditcommissie. Een crisis rondom misstanden en onregelmatigheden brengt mogelijk ook persoonlijke reputatie- en aansprakelijkheidsrisico's met zich mee voor de raad van commissarissen en daarmee voor de auditcommissie.

Hoog afbreukrisico

Als de organisatie in een crisis terechtkomt, stellen stakeholders vaak direct de vraag: waar was de raad van commissarissen?

Natuurlijke rol auditcommissie bij een crisis

Toezicht houden op het bestuur bij een crisis is een verantwoordelijkheid van de volledige raad van commissarissen. De raad doet hierbij echter vaak een beroep op de auditcommissie. Een logische keuze, gezien de taakstelling van de auditcommissie: toezicht op de interne controle, materiële risico's en onzekerheden en de kwaliteit en integriteit van de financiële verslaggeving. De auditcommissie kan ook namens de raad van commissarissen leiding geven aan een onderzoek naar de gang van zaken bij (vermoedens van) misstanden of onregelmatigheden waarbij mogelijk (een lid van) het bestuur of het senior management direct of indirect betrokken is. Onder indirecte betrokkenheid valt ook 'wegkijken', of verzuimen om passende

maatregelen te nemen bij signalen van misstanden of onregelmatigheden. De auditcommissie speelt eveneens een belangrijke rol bij het toezicht op het herstelplan en/of het crisisplan, als de continuïteit van de organisatie moet worden veiliggesteld.

Toezicht op maat

Elke crisis is weer anders en vraagt om maatwerk. Een blauwdruk voor goed toezicht in een crisissituatie bestaat niet: het hanteren van 'stappenplannen' biedt slechts schijnzekerheid en vergroot het gevaar dat de focus komt te liggen op het winnen van de vorige oorlog. De auditcommissie kan zich echter wel voorbereiden op de eigen rol als de organisatie in een crisis terechtkomt, de dilemma's daarbij en de do's and don'ts. Oefen met een gesimuleerde situatie en investeer in de onderlinge verhoudingen als de zon schijnt, zodat er een sterk team staat als de storm opsteekt.

Als een crisis niet meer kan worden voorkomen

Het toezicht van de raad van commissarissen en de auditcommissie is primair gericht op het waar mogelijk voorkomen van misstanden en onregelmatigheden door goed toezicht op effectieve interne risicobeheersings- en controlesystemen en een gezonde cultuur en door voortdurende alertheid op waarschuwingstekens. Het vroegtijdig signaleren van integriteitsrisico's komt uitgebreid aan de orde in hoofdstuk 4 (Control & Compliance) en hoofdstuk 5 (Cultuur en gedrag). Dit hoofdstuk is gericht op de rol

In dit hoofdstuk komen de volgende onderwerpen aan de orde:

1. Meldingen van misstanden en onregelmatigheden
2. Wanneer een onderzoek en door wie?
3. Het samenstellen van het onderzoeksteam
4. Bepalen scope en procedures van het onderzoek
5. De uitvoering van het onderzoek
6. Communiceren over de voortgang van het onderzoek
7. Eindrapportage en het herstelplan
8. Na de crisis: trek de lessen



van de auditcommissie wanneer er toch een specifieke situatie ontstaat als gevolg van onvoorziene of te laat gesignaleerde misstanden en onregelmatigheden of integriteitsproblemen.

1. Meldingen van misstanden en onregelmatigheden

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Ondanks hun toezicht en alertheid op signalen van een ongezonde cultuur en integriteitsschendingen, worden raden van commissarissen soms toch geconfronteerd met misstanden en onregelmatigheden. De afgelopen jaren hebben daarvan voldoende voorbeelden te zien gegeven. Fraude en corruptie bijvoorbeeld zijn vaak moeilijk te detecteren. Degenen die zich er schuldig aan maken, doen immers hun uiterste best om hun handelen te verhullen. Bovendien is het vanuit de top van de organisatie moeilijk om de hele (internationale) organisatie te overzien. Dat geldt zeker voor de raad van commissarissen en daarmee voor de auditcommissie, die als toezichthouders op afstand staan. Ook voor Internal Audit en de externe accountant blijkt het soms lastig om fraude en andere misstanden te identificeren, zoals het niet voldoen aan wet- en regelgeving, (boekhoud)fraude, corruptie, witwassen, belangenverstrengeling, grensoverschrijdend gedrag, klachten over onheuse bejegening, of andere vormen van ongewenst of zelfs crimineel gedrag.

Formele kanalen en het informele circuit
Misstanden en onregelmatigheden kunnen op verschillende manieren aan het licht komen: zowel via formele als informele kanalen en zowel via interne als externe bronnen. Zo kunnen medewerkers voor het doen van een melding gebruikmaken van de klokkenluidersregeling (zie hoofdstuk 5 over cultuur en gedrag voor het als auditcommissie toetsen daarvan) of de vertrouwenspersoon. Ook Internal Audit, de compliance-officer of de verantwoordelijke

functionaris voor integriteitsbeleid kan misstanden en onregelmatigheden vermoeden of constateren en melden. Klanten of leveranciers kunnen een officiële klacht indienen, partijen kunnen een claim indienen of een rechtszaak aanspannen, of een extern toezichthouder/bevoegde instantie kan een afwijking van de regels vaststellen. Organisaties worden echter ook vaak geconfronteerd met het informele circuit: zo kunnen misstanden naar buiten komen via geruchtenvorming op sociale media, lekken naar de pers en/of als gevolg van onderzoeksjournalistiek, of via anonieme tips van externe betrokkenen.

Materieel versus niet-materieel
Als er sprake is van (een vermoeden van) materiële misstanden en onregelmatigheden, dan wordt het bestuur geacht dat onmiddellijk te melden aan de voorzitter van de raad van commissarissen, volgens de Code. Als het functioneren van een bestuurder daarbij in het geding is, kan een werknemer dit ook rechtstreeks melden aan de voorzitter van de raad van commissarissen. De Code spreekt dus over materiële misstanden en onregelmatigheden: dat impliceert dat niet álle misstanden en onregelmatigheden hoeven te worden gemeld aan de raad van commissarissen. Het betreft alleen de issues met mogelijk belangrijke impact, die het bedrijf forse schade kunnen toebrengen, bijvoorbeeld in termen van geld of reputatie. De auditcommissie kan de materialiteit van misstanden en onregelmatigheden echter anders definiëren dan het bestuur. In dat geval worden

onoorbare zaken door het bestuur mogelijk niet gemeld, waarvan de auditcommissie wél op de hoogte wil zijn voor een eigen risico-inschatting.

Leg afspraken over melding en de materialiteit van issues vast
Een effectieve auditcommissie maakt de eigen definitie van materialiteit dan ook duidelijk kenbaar aan het bestuur en maakt heldere afspraken over wanneer welke issues door het bestuur gemeld worden. Dat zal in elk geval gaan om zaken die effect hebben op de financiële en niet-financiële rapportage, de positie van het bestuur, potentiële media-aandacht, de interne audit en de externe audit. Op basis daarvan kan de auditcommissie en de gehele raad van commissarissen inschatten of een onderzoek moet plaatsvinden en door wie dat uitgevoerd kan worden, in hoeverre intensief toezicht benodigd is op het aanpakken van de kwesties door het bestuur en of eigen bemoeienis of ingrijpen gewenst is. Het is goed om deze zaken vast te leggen.

Vraag om rechtstreekse rapportage door de direct verantwoordelijke functionarissen
Vraag als auditcommissie ook om een rechtstreekse rapportage door de direct verantwoordelijke functionarissen van alle door hen ontvangen meldingen: hoe zijn deze onderzocht en afgehandeld?

Bepaal de materialiteit en de noodzaak van toezicht door de auditcommissie

De materialiteit van misstanden en onregelmatigheden kan worden gebaseerd op:

- **kwantitatieve materialiteit:** mogelijke gevolgen voor financiële en niet-financiële rapportage en/of blijk gevend van een zwakke plek in de interne controle;
- **kwalitatieve materialiteit:** mogelijke schade aan merk of reputatie;
- **ernst vanuit compliance- of ethisch oogpunt:** de niet-naleving van wet- en regelgeving, het niet voldoen aan maatschappelijke normen en/of het mogelijk optreden door externe toezichthouders en het Openbaar Ministerie;
- **reikwijdte:** betrokkenheid van senior management en managers/medewerkers in de financiële kolom of een ongezonde cultuur in de organisatie;
- **reactie:** een niet-adequate opvolging door het bestuur of een gebrek aan objectiviteit of transparantie;
- **complexiteit:** het management slaagt er niet in de kwestie tijdig en adequaat op te lossen.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Vraag daarbij om rapportage op regelmatige basis, bijvoorbeeld eenmaal per kwartaal of halfjaar en ten minste eenmaal per jaar. Dat werkt niet alleen disciplinerend, maar op die manier kan de auditcommissie zich ook een oordeel vormen over de cultuur van de organisatie, de toon aan de top en de effectiviteit van de klokkenluidersregeling en andere procedures voor het melden van misstanden en onregelmatigheden (bijvoorbeeld als er weinig wordt gemeld).

Melding door de externe accountant
Naast de eerdergenoemde interne en externe bronnen, kunnen misstanden en onregelmatigheden ook ontdekt of vermoed worden door de externe accountant. Deze zal aanwijzingen of de constatering van fraude of andere misstanden of onregelmatigheden aan de bestuurders en/of de commissarissen melden. De voorzitter van de auditcommissie wordt in elk geval onmiddellijk geïnformeerd. Deze informeert daarna direct de andere commissarissen. De externe accountant vormt dus een rechtstreekse informatiebron voor de auditcommissie voor de melding van materiële misstanden en onregelmatigheden, onafhankelijk van het bestuur.

Wederzijds informeren
Wanneer (het vermoeden van) een misstand of onregelmatigheid het functioneren van een bestuurder betreft, dan meldt de externe accountant dit niet (ook) aan het bestuur, maar rechtstreeks aan de voorzitter van de raad van commissarissen. Wanneer de organisatie zelf

misstanden en onregelmatigheden ontdekt, of hierop wordt gewezen door bevoegde instanties, dan zal ook de externe accountant op de hoogte worden gesteld.

Incident of systematisch frauduleus handelen?
Bij (het vermoeden van) fraude of andere misstanden zal de externe accountant actie ondernemen, ongeacht de materialiteit. Zo is de accountant geïnteresseerd in de vraag of er sprake is van een incident, of systematisch frauduleus handelen. De accountant geeft aan welke actie

- ‘We vermoeden dat...’**
De externe accountant bespreekt aanwijzingen van fraude in elk geval met de auditcommissie/de raad van commissarissen in de volgende situaties:
- het bestuur is zelf (mogelijk) betrokken bij de fraude;
 - het bestuur treft geen toereikende maatregelen om de fraude ongedaan te maken en om herhaling te voorkomen;
 - de gevolgen zijn van materieel belang voor de financiële verslaggeving.

Bespreek vooraf met de externe accountant hoe, wanneer en in welke volgorde hij/zij bij een (vermoeden) van fraude of andere misstanden contact opneemt met de auditcommissie.

de organisatie ten minste moet ondernemen. De organisatie is zelf verantwoordelijk voor het onderzoek naar de aard en omvang van de fraude. Wel blijft de externe accountant betrokken bij het onderzoek. Er kan immers informatie aan het licht komen die de accountant nodig heeft om de impact op de jaarrekening en het eventuele herstelplan te kunnen beoordelen en om de controle te kunnen afronden. De accountant kan de controle namelijk niet afronden, zolang onduidelijk is of uit het onderzoek een materiële correctie op de jaarrekening voortvloeit, of zolang onduidelijk is of het bestuur betrokken is bij de fraude of de misstand. Zo kan de accountant niet steunen op een bevestiging bij de jaarrekening (**letter of representation**) aan het einde van de controle, als blijkt dat degene die deze bevestiging ondertekent – vaak (een lid van) het bestuur – niet integer is.

Melding aan externe instanties
Naast de verantwoordelijkheid voor het intern melden van (vermoedens van) misstanden en onregelmatigheden aan het bestuur en/of de voorzitters van de auditcommissie of raad van commissarissen, heeft de externe accountant soms de plicht om deze (ook) te melden aan externe instanties (zie volgende pagina). Het is goed gebruik dat de externe accountant het bestuur en de auditcommissie op de hoogte stelt van externe meldingen. Uitzondering daarop vormt de melding van ongebruikelijke transacties: daarvoor geldt een wettelijke geheimhoudingsplicht. De externe accountant mag dus niet communiceren of hij

een ongebruikelijke transactie wel of niet heeft gemeld aan de Financial Intelligence Unit-Nederland (FIU-Nederland).

Hoe reageren wanneer externe toezichthouders, bevoegde instanties of opsporingsdiensten zich melden?
Een melding van de externe accountant, de organisatie zelf of andere partijen binnen of buiten de organisatie kan leiden tot een verzoek om nadere informatie, een onderzoek of zelfs een ‘inval’ van externe toezichthouders, bevoegde instanties of opsporingsdiensten (zoals het Openbaar Ministerie, de Fiscale inlichtingen- en opsporingsdienst (FIOD), de Autoriteit Financiële Markten (AFM), de Autoriteit Consument & Markt (ACM), de Nederlandse Zorgautoriteit (NZa), et cetera. Best practice is dat de auditcommissie daarover wordt geïnformeerd door het bestuur en de medewerking van het bestuur aan het onderzoek en de voortgang daarvan monitort.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Externe meldingen door de externe accountant

Melding aan de Autoriteit Financiële Markten (AFM)

De externe accountant doet een melding bij de AFM wanneer hij of zij bij een OOB – al dan niet in relatie tot een (vermoeden van) fraude of andere misstanden – de volgende zaken constateert:

- Er is sprake van een materiële inbreuk op de wettelijke of bestuursrechtelijke bepalingen die, in voorkomend geval, de voorwaarden voor toelating regelen of die specifiek de activiteiten van de organisatie van openbaar belang regelen.
- Er is sprake van een materiële bedreiging voor of twijfel over de continuïteit.
- Er zal een niet-goedkeurende controleverklaring afgegeven worden.

Ook zijn externe accountants verplicht een tussentijdse beëindiging van een wettelijke controleopdracht – om welke reden dan ook – te melden bij de AFM.

Melding ongebruikelijke transacties bij de Financial Intelligence Unit-Nederland (FIU-Nederland)

De externe accountant heeft volgens de Wwft (Wet ter voorkoming van witwassen en financieren van terrorisme) de plicht om ongebruikelijke transacties te melden. Dit zijn transacties en geldstromen die te relateren zijn aan witwassen, financiering van terrorisme of onderliggende misdrijven. Accountants melden geconstateerde ongebruikelijke transacties in alle omstandigheden zo snel mogelijk bij FIU-Nederland. De accountant kan ook een melding doen als hij of zij aanleiding heeft om te veronderstellen dat transacties verband kunnen houden met witwassen of financieren van terrorisme. De accountant licht de reden voor de melding toe bij FIU-Nederland, maar hoeft deze niet

te ondersteunen met bewijsvoering. De FIU-Nederland analyseert meldingen en bepaalt welke meldingen doorgegeven worden aan opsporingsdiensten.

De externe accountant stelt de organisatie waar ongebruikelijke transacties zijn geconstateerd of worden verondersteld, niet op de hoogte van de melding. De wet vereist dat de melding plaatsvindt onder geheimhouding: de externe accountant mag deze dus niet bespreken met het bestuur of de raad van commissarissen/de auditcommissie.

Melding materiële fraude bij de Nationale Politie

Een externe accountant die tijdens het verrichten van een wettelijke controle de beschikking krijgt over gegevens of inlichtingen die het redelijk vermoeden rechtvaardigen dat sprake is van fraude van materieel belang ten aanzien van de financiële verantwoording van de controleklant, meldt dit aan aan de Nationale Politie.

Deze melding kan achterwege blijven indien:

- (a) de controleklant, nadat de externe accountant deze heeft gewezen op een redelijk vermoeden van fraude van materieel belang, daarnaar onverwijld onderzoek verricht of doet verrichten en op basis daarvan een schriftelijk plan opstelt waarin zijn opgenomen:
 - (1) de maatregelen die de controleklant zal nemen om de gevolgen van de fraude, voor zover mogelijk, ongedaan te maken en om herhaling van de fraude te voorkomen; en
 - (2) de termijn waarbinnen de controleklant de bedoelde maatregelen zal hebben uitgevoerd;
- (b) de externe accountant, binnen vier weken nadat het plan is opgesteld, heeft geoordeeld dat het in onderdeel a bedoelde plan toereikend is; en

- (c) de externe accountant heeft vastgesteld dat de controleklant de in het plan opgenomen maatregelen binnen de genoemde termijn in voldoende mate heeft uitgevoerd.

Melding niet-naleving wet- en regelgeving (NOCLAR) bij bevoegde instantie

De accountantsorganisatie meldt geconstateerde, mogelijke of dreigende niet-naleving van wet- en regelgeving (Non-Compliance with Laws and Regulations – NOCLAR) onmiddellijk aan een bevoegde instantie, als direct handelen door de desbetreffende instantie noodzakelijk lijkt om aanzienlijke schade te voorkomen of te beperken. Onder aanzienlijke schade wordt verstaan: ernstige nadelige gevolgen voor de accountantsorganisatie zelf, de gecontroleerde organisatie, medewerkers, beleggers, schuldeisers, andere stakeholders en de maatschappij in het algemeen. Als de organisatie zelf de wettelijke plicht heeft om niet-naleving aan een bevoegde instantie te melden, zal de externe accountant daarop aandringen.

De accountant zal geen melding doen van het niet naleven van wet- en regelgeving als deze ‘duidelijk onbetekenend’ is, of als er redelijkerwijs op vertrouwd mag worden dat de procedure van de organisatie voor het reageren op niet-naleving toereikend is. De externe accountant zal geconstateerde, mogelijke of dreigende niet-naleving bespreken met de opdrachtgever – zijnde de raad van commissarissen – en eventueel met het verantwoordelijke management, de governance-functionarissen en Internal Audit van de organisatie. De accountant zal daarbij aandringen op het zo spoedig mogelijk nemen van maatregelen om (herhaling van) niet-naleving te voorkomen of te herstellen en de gevolgen ervan zoveel mogelijk weg te nemen.

■ **Rol van de auditcommissie bij NOCLAR**

De auditcommissie ondersteunt de raad van commissarissen bij het toezicht op nalevings(risico’s). Er ligt dus een belangrijke rol voor de auditcommissie bij NOCLAR: adequaat toezien op de opzet en werking van de interne risicobeheersings- en controlesystemen die gericht zijn op het voorkomen van niet-naleving. De auditcommissie zal de effectiviteit daarvan nauwgezet monitoren, vooral in een gereguleerde omgeving waarin wet- en regelgeving sterk aan verandering onderhevig is. Wanneer er toch niet-naleving dreigt of wordt geconstateerd, dan ziet de auditcommissie erop toe dat het bestuur de aanbevelingen en opmerkingen van de externe accountant naleeft om de schade zo veel mogelijk te beperken. Door proactief te handelen en de regie te nemen ten aanzien van de naleving van wet- en regelgeving, kan de auditcommissie een melding aan een bevoegde instantie – door de organisatie of door de externe accountant – wellicht helpen voorkomen.



2. Wanneer een onderzoek en door wie?

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

1. Meldingen van misstanden en onregelmatigheden
2. Wanneer een onderzoek en door wie?
3. Het samenstellen van het onderzoeksteam
4. Bepalen scope en procedures van het onderzoek
5. De uitvoering van het onderzoek
6. Communiceren over de voortgang van het onderzoek
7. Eindrapportage en het herstelplan
8. Na de crisis: trek de lessen

9. Communicatie

Signalen van misstanden en onregelmatigheden vragen om onafhankelijk onderzoek. De raad van commissarissen ziet toe op het onderzoek door het bestuur en op een adequate opvolging van eventuele aanbevelingen tot herstelacties, als er inderdaad een misstand of onregelmatigheid is geconstateerd. Als het bestuur daar zelf bij betrokken is, neemt de raad van commissarissen het initiatief voor een onderzoek en de aansturing daarvan. Op die manier is de onafhankelijkheid van het onderzoek gewaarborgd. Dat kan overigens tot gespannen verhoudingen met het bestuur leiden. Door van tevoren – wanneer er nog geen sprake is van (het vermoeden van) misstanden en onregelmatigheden – met de bestuurders te bespreken onder welke omstandigheden de raad van commissarissen een onderzoek instelt, wordt duidelijkheid gecreëerd. Tenslotte is het voor bestuurders ook belangrijk om officieel vrijgepleit te worden van betrokkenheid bij misstanden en onregelmatigheden als ze niets fout hebben gedaan. Zonder onafhankelijk onderzoek blijft de mogelijke verdenking wellicht bestaan.

Auditcommissie of crisiscommissie?

Afhankelijk van de situatie, kan de raad van commissarissen het toezicht op het onderzoek delegeren aan de auditcommissie. Als bij een of meer leden van de auditcommissie sprake is van belangenverstrengeling, of als andere commissarissen over meer ervaring met crisismanagement beschikken, kan de raad van commissarissen een speciale crisiscommissie in het leven roepen. Ook kan een commissaris met

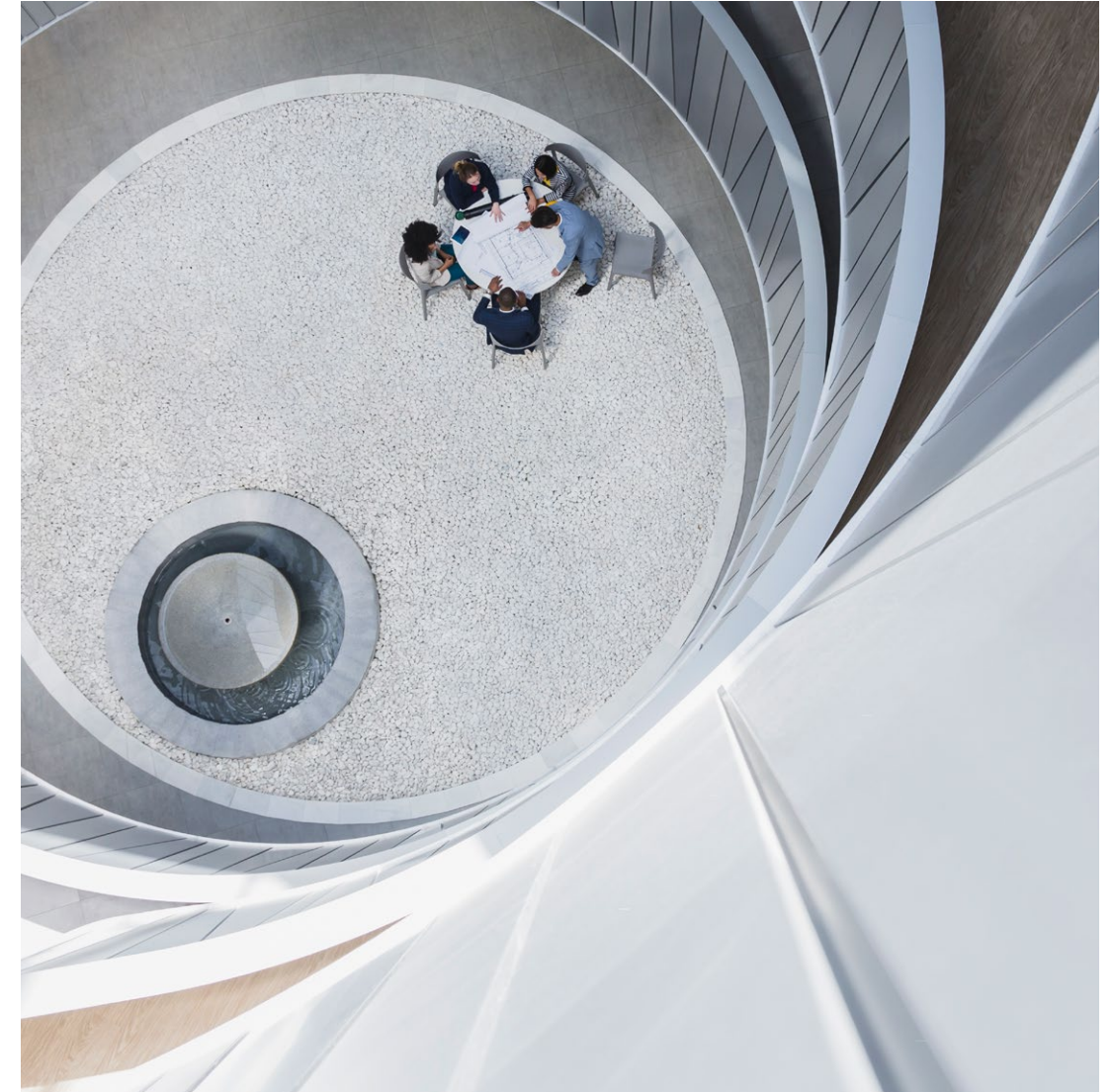
specialistische expertise worden toegevoegd aan de auditcommissie of de crisiscommissie, bijvoorbeeld ervaring met cybersecurity bij een cyberaanval. In dit hoofdstuk concentreren we ons op de rol van de auditcommissie.

Crisisbestendigheid gevraagd

Het managen van een crisis gaat gepaard met lastige beslissingen onder grote tijdsdruk en vraagt om goede communicatie met de aandeelhouders, de externe accountant, relevante belanghebbenden (zoals de ondernemingsraad, leveranciers en banken) en mogelijk ook externe toezichthouders. Van groot belang is dat de auditcommissie opgewassen is tegen de situatie en beschikt over onafhankelijkheid, crisiservaring, een gezonde dosis scepsis, integriteit en sterke communicatieve vaardigheden. De rol van de voorzitter is daarbij cruciaal.

Is het bestuur of de raad van commissarissen leidend?

Hoe ernstiger de aantijgingen of potentiële gevolgen, hoe actiever de rol van de raad van commissarissen/auditcommissie in het toezicht op of het aansturen van het onderzoek en het bepalen van de benodigde inzet van mensen en middelen. Van de auditcommissie wordt bijvoorbeeld een leidende rol verwacht bij crises die gevolgen hebben voor de financiële en niet-financiële rapportages, de externe audit en potentiële media-aandacht en in elk geval wanneer de positie van het bestuur en senior management – de cfo en de financiële kolom in het bijzonder – in het geding is.



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Vragen voor de auditcommissie bij een onderzoek naar misstanden en onregelmatigheden door het bestuur:

- Hoe weten we of het bestuur de signalen of meldingen adequaat opvolgt?
- Hoe gedetailleerd willen we daarvan door het bestuur op de hoogte gehouden worden?
- Wanneer komt de auditcommissie (alsnog) zelf in actie?

Intern onderzoek...
Een belangrijke vraag voor de auditcommissie is of het onderzoek intern kan plaatsvinden, of beter

bij een externe partij kan worden neergelegd. Het antwoord op de vraag naar intern of extern onderzoek is afhankelijk van de ernst en de gevoeligheid van de aantijgingen. Bij zaken van minder grote betekenis (of waarbij lager management of externe partijen zijn betrokken) kan voor een intern onderzoek worden gekozen door Internal Audit en/of het juridische team en/of het complianceteam. Voorwaarde is dat het team beschikt over voldoende kennis, ervaring en capaciteit voor een dergelijk onderzoek. Ook is van belang dat het onderzoeksteam voldoende onafhankelijk is van het controleobject en de mogelijk betrokkenen. De teams kennen de organisatie goed en kunnen daardoor tijd en geld besparen bij het onderzoek. Maar dit argument gaat niet op als niet aan de overige

voorwaarden is voldaan. Het onderzoeksteam kan rapporteren aan het bestuur, dat vervolgens de auditcommissie informeert. Een effectieve auditcommissie houdt in dat geval wel de vinger aan de pols. Een nadeel van een intern onderzoek is de externe legitimiteit van het onderzoek. De buitenwereld plaatst namelijk al snel vraagtekens bij de onafhankelijkheid van een intern onderzoek.

... of extern onderzoek?
Bij zaken van grote betekenis en bij betrokkenheid van het hoger management en het bestuur, zal de auditcommissie doorgaans een extern onderzoek laten uitvoeren. Daarmee wordt voorzien in de externe objectiviteit en ervaring die regelgevende instanties en externe toezichthouders eisen en door de media en het grote publiek wordt gevraagd. Het onderzoeksteam rapporteert rechtstreeks aan de auditcommissie, die vervolgens de raad van commissarissen aangesloten houdt.

In de praktijk wordt dat vaker dan voorheen gekozen voor een extern onderzoek. Afwegingen (zie kader) als de gepercipieerde objectiviteit en daarmee de geloofwaardigheid, alsmede de mogelijke impact van een intern onderzoek op de toekomstige positie in de organisatie van interne onderzoekers, spelen een rol in die keuze.



Intern of extern onderzoek?
De auditcommissie kan de volgende vragen stellen:

- Wie is in deze specifieke situatie de juiste partij voor het initiëren en aansturen van het onderzoek: het bestuur of de raad van commissarissen (via de auditcommissie)?
- Kan het onderzoek intern plaatsvinden of wordt een externe partij ingeschakeld? Hierbij is relevant of de benodigde specifieke kennis en ervaring in voldoende mate aanwezig is en of het onderzoek onafhankelijk (in wezen en in schijn) van mogelijke betrokkenen kan plaatsvinden.
- Is intern voldoende juridische expertise voorhanden (bedrijfsjurist, General Counsel), of is het beter om deze extern in te huren?
- Hoe geloofwaardig is een intern onderzoek versus een extern onderzoek in de ogen van buitenstaanders?
- Is in de afwegingen rondom een intern onderzoek meegewogen wat de mogelijke effecten kunnen zijn op de toekomstige positie in de organisatie van functionarissen die het onderzoek uitvoeren?



3. Het samenstellen van het onderzoeksteam

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis
 1. Meldingen van misstanden en onregelmatigheden
 2. Wanneer een onderzoek en door wie?
 3. Het samenstellen van het onderzoeksteam
 4. Bepalen scope en procedures van het onderzoek
 5. De uitvoering van het onderzoek
 6. Communiceren over de voortgang van het onderzoek
 7. Eindrapportage en het herstelplan
 8. Na de crisis: trek de lessen
9. Communicatie

De samenstelling van het onderzoeksteam wordt bepaald op basis van de eerste inschatting van de ernst van de situatie en de vraag of senior management eventueel betrokken zou kunnen zijn. Een goed onderzoeksteam kenmerkt zich door objectiviteit en voldoende materie- of dossierkennis en is volledig berekend voor de uitdagende en vaak gevoelige taak. De auditcommissie selecteert de juiste partij om het onderzoek te leiden. Daarnaast wordt de externe accountant gevraagd om instemming met de gemaakte keuze, om te voorkomen dat achteraf discussie ontstaat over de onafhankelijkheid van het onderzoek. Een intern onderzoeksteam bestaat vaak uit Internal Audit en/of het juridische en complianceteam. Een extern onderzoeksteam wordt vaak aangevoerd door een advocatenkantoor, dat vervolgens opdrachten kan verstrekken aan forensische expertise of andere specialisten. Op deze wijze kan het gehele team vallen onder het verschoningsrecht van de advocaat die de leiding heeft over het onderzoek (zie kader **Legal privilege**).

Autoriteit, draagvlak en crisiservaring

Belangrijk is dat de partij die het onderzoek leidt, beschikt over autoriteit, draagvlak, expertise en ervaring in de uitvoering van vergelijkbare onderzoeken en het vinden van de juiste balans tussen snelheid, efficiency, diepgang en grondigheid. Voorkomen moet worden dat het onderzoek opnieuw moet worden gedaan, omdat het niet blijkt te voldoen aan formele en maatschappelijke maatstaven of aan de eisen die

Best practice

Kies niet voor de huisadvocaat om het onderzoek naar misstanden en onregelmatigheden te leiden. De bestaande relatie van de eigen juridisch adviseur met de organisatie en het bestuur kan gevolgen hebben voor de objectiviteit of de perceptie daarvan door de buitenwereld. Het onderzoek moet niet alleen de belangen van de onderneming (zoals de eigen rechtspositie) behartigen, maar ook die van een bredere groep stakeholders. Een onafhankelijke samenstelling en opstelling van het onderzoeksteam is dan ook een voorwaarde. De externe accountant zal de onafhankelijkheid van de onderzoekende partij ook meenemen en wegen in de beoordeling van het verloop en de uitkomsten van het onderzoek.



de externe accountant aan de onderzoekende partij stelt.



'Legal privilege'

Vaak wordt een extern onderzoek uitgevoerd door of onder leiding van een advocatenkantoor dat is gespecialiseerd in integriteitsonderzoeken. Aan dit externe legalteam kunnen – afhankelijk van de aard van het onderzoek – specialisten worden toegevoegd, zoals forensische accountants of andere materiedeskundigen. Een advocatenkantoor kan onder **legal privilege** (verschoningsrecht) werken. Dit houdt in dat het onderzoeksrapport niet aan derden hoeft te worden verstrekt, anders dan aan het bestuur en/of de raad van commissarissen. De accountant zal in overeenstemming met zijn of haar verantwoordelijkheid wel inzage in het rapport verlangen.

4. Bepalen juiste scope en onderzoeksaanpak

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Na de beslissing over het toezicht op het onderzoek en de samenstelling van het onderzoeksteam, wordt de scope van het onderzoek bepaald. Het is van belang dat de voorgestelde onderzoeksaanpak/methodologie past bij de aanleiding en probleemstelling. De reikwijdte van het onderzoek is zodanig dat antwoord kan worden gegeven op de volgende vragen:

- Wie zijn er betrokken geweest bij de misstand of onregelmatigheid?
- Welke maatregelen worden genomen, zowel in repressieve zin (naar betrokkenen) als in preventieve zin (om te voorkomen dat het nog eens gebeurt)?
- Kan het onderzoek zich beperken tot het betrokken individu, team of bedrijfsonderdeel, of wordt vermoed dat er sprake is van een organisatiebreed risico? Anders gesteld: is er sprake van een incident, of lijken de geconstateerde misstanden en onregelmatigheden uiting van een ongezonde cultuur? In dat geval zal opschaling van het onderzoek plaatsvinden.
- Welke controlemaatregelen hebben gefaald en welke maatregelen worden genomen om herhaling te voorkomen?
- Wat is de eventuele (financiële) schade en de impact op de jaarrekening? Is het noodzakelijk om deze te corrigeren?

Balanceren tussen zorgvuldigheid en snelheid

Een juiste onderzoekscope kan vertragingen, hoge kosten en het ontstaan van extra schade tijdens het onderzoek voorkomen. De auditcommissie zal dus zorgvuldigheid betrachten bij het bepalen van de scope en de onderzoeksaanpak en niet toegeven aan de (tijds) druk die aandeelhouders en andere stakeholders kunnen uitoefenen op het proces. Aan de andere kant is snelheid geboden. Het is daarom de kunst om als auditcommissie hierin de juiste balans te vinden.

Te brede of te smalle scope

Het hanteren van een te brede scope en onderzoeksaanpak kan veel tijd en geld kosten, een te smalle scope en aanpak op de lange termijn eveneens. Bijvoorbeeld in de vorm van reputatieschade, wanneer de misstanden en onregelmatigheden na de presentatie van de onderzoeksresultaten toch veelomvattender blijken te zijn dan gedacht. De scope en aanpak kunnen ook tijdens het onderzoek veranderen, afhankelijk van de bevindingen. De auditcommissie houdt zich dus niet alleen aan het begin van het onderzoek bezig met het bepalen van de scope en de aanpak, maar houdt ook nauwlettend in de gaten of deze bijstelling behoeven gedurende het onderzoek. De auditcommissie vraagt hiervoor ook om akkoord van de externe accountant voor zover het onderzoek zijn of haar controle raakt. Beide partijen hebben belang bij een goed uitgevoerd onderzoek.

Valkuilen bij het bepalen van de scope

Het gevaar bestaat dat een misstand of onregelmatigheid wordt onderschat of gebagatelliseerd door de (betrokken) partijen of personen. Ook is het moeilijk voor de raad van commissarissen – en dus ook voor de auditcommissie – om een (fraude)onderzoek in te stellen naar bestuurders of senior managers met wie men al jaren nauw samenwerkt en denkt een (vertrouwens)band te hebben opgebouwd. De raad van commissarissen of auditcommissie kan ook opzien tegen de kosten van een onderzoek met een bredere scope. Bedenk dat de schade achteraf veel groter kan zijn als aan het begin van het onderzoek geen adequate scope wordt bepaald.

Vijf oorzaken van vertraging tijdens het onderzoek naar misstanden en onregelmatigheden

				
De aanvankelijke scope blijkt te smal of te breed.	De organisatie heeft onvoldoende capaciteit en middelen voor het verkrijgen van de benodigde documenten en rapportages.	De organisatie is niet in staat om een ervaren externe partij aan te trekken die het onderzoek kan uitvoeren.	Het onderzoek vraagt om complexe en tijdrovende forensische expertise.	Het onderzoeksteam communiceert de resultaten mondeling in plaats van schriftelijk, waardoor het bestuur en de externe accountant na afloop van het onderzoek gedwongen worden om zich bezig te houden met documentatie- en dossiervorming.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

5. De uitvoering van het onderzoek

Een onderzoek naar misstanden en onregelmatigheden bestaat – afhankelijk van de gekozen scope en aanpak – uit het screenen van documenten, e-mailwisselingen, WhatsApps en telefoonverkeer, digitale bestanden, boekenonderzoek en interviews met betrokkenen. De organisatie wordt geacht alle relevante informatie voor het onderzoek te overleggen en te bewaren, ook als deze belastend is. De organisatie moet ook kunnen aantonen hoe het onderzoek is uitgevoerd en welke informatie onderzocht is. Het advocatenkantoor dat het onderzoek leidt kan aangeven welke informatie bewaard moet worden, zodra het onderzoek is begonnen. Van belang is dat de (digitale) informatie zo snel mogelijk wordt veiliggesteld, voordat mogelijk in het onderzoek betrokken personen daarover

worden geïnformeerd. Op die manier is de kans minimaal dat relevante informatie wordt gewist of gemanipuleerd.

Wees consequent

Bij een onderzoek naar misstanden en onregelmatigheden is gelijke behandeling van alle medewerkers essentieel. Vermijd (de schijn) dat sommige managers of medewerkers een voorkeursbehandeling krijgen of dat inconsistent wordt omgegaan met ongewenst gedrag. Inconsequent gedrag ondermijnt de cultuur en maakt de kans minder groot dat medewerkers in de toekomst misstanden en onregelmatigheden melden.

Best practices

- Onderneem snel actie om verdere (reputatie)schade te voorkomen.
- Stel belangrijke informatie en bewijsvoering snel veilig.
- Wees consistent in het onderzoeken van alle misstanden en onregelmatigheden en handel daarbij strikt volgens het bedrijfsbeleid, onafhankelijk van het organisatieniveau waarop de betrokken persoon werkzaam is.
- Wees je ervan bewust dat alle medewerkers die een melding van misstanden en onregelmatigheden hebben gedaan, externe klokkenluiders kunnen worden. Zie erop toe dat elke melding adequaat wordt opgevolgd en de genomen maatregelen en getrokken conclusies goed worden gedocumenteerd.
- Vraag als auditcommissie om periodieke informatie over materiële misstanden en onregelmatigheden (en definieer daarbij het niveau van materialiteit).
- Overweeg of het noodzakelijk is om stakeholders op de hoogte te stellen van het onderzoek, de voortgang en de uitkomsten.

Gangbare onderzoeksprocedures



Identificeren en beoordelen van documenten



Elektronisch onderzoeken van digitale informatie (zoals harde schijven en WhatsApps)



Interviews



Beoordelen en analyseren van rapportages

Valkuilen bij onderzoeken

- aannemen dat een intern onderzoek alle betrokken partijen en toezichthouders tevreden zal stellen en geen externe expertise aantrekken;
- externe onderzoekers aanstellen die niet over de juiste expertise beschikken, of niet geloofwaardig en onafhankelijk zijn;
- niet (tijdig) overleggen met bevoegde instanties, externe toezichthouders of de externe accountant over de scope van het onderzoek en vervolgens moeite hebben deze partijen te overtuigen om vertrouwen te hebben in de resultaten van het onderzoek;
- een niet-adequaat onderzoek (laten) uitvoeren, waardoor de geloofwaardigheid van de organisatie nog meer onder druk komt te staan;
- niet of onvoldoende de gevolgde onderzoeks aanpak vastleggen, waardoor de organisatie niet in staat is om de resultaten van het onderzoek te verdedigen;
- het onderzoek te gehaast uitvoeren, terwijl een te weinig diepgaand onderzoek de partijen niet tevreden zal stellen;
- toestaan dat het bestuur te veel wordt opgeslokt door het onderzoek en daardoor de focus verliest op het leiden van het bedrijf;
- het verliezen van een objectieve houding ten aanzien van het bestuur en geen maatregelen nemen wanneer de noodzaak daartoe wel naar voren komt uit het onderzoek.

6. Communiceren over de voortgang en bevindingen van het onderzoek

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

1. Meldingen van misstanden en onregelmatigheden
2. Wanneer een onderzoek en door wie?
3. Het samenstellen van het onderzoeksteam
4. Bepalen scope en procedures van het onderzoek
5. De uitvoering van het onderzoek
6. Communiceren over de voortgang van het onderzoek
7. Eindrapportage en het herstelplan
8. Na de crisis: trek de lessen

9. Communicatie

De auditcommissie wordt door het onderzoeksteam op de hoogte gebracht van de voortgang van het onderzoek en de tussentijdse bevindingen. De auditcommissie informeert op haar beurt de raad van commissarissen over de voortgang en eventuele voorlopige resultaten. Ook het bestuur en het management worden regelmatig geïnformeerd. Zij hebben behoefte aan tussentijdse informatie over het onderzoek om hun taken goed te kunnen uitvoeren en plannen. Denk aan zaken als de verwachte duur van het onderzoek, de medewerkers die daarvoor nodig zijn en het te verwachten effect op de financiële verslaglegging. De auditcommissie zorgt er bij het communiceren over het onderzoek overigens voor dat informatie over de scope, aanpak en tussentijdse bevindingen niet wordt gedeeld met potentiële getuigen of verdachten. De externe accountant blijft betrokken bij het onderzoek naar de aard en omvang van de fraude en wordt dus ook op de hoogte gehouden.

Best practice

Belangrijk in een crisis is proactief en intensief te communiceren.. Zorg dat je als voorzitter van de auditcommissie goed bereikbaar bent en snel en veelvuldig schakelt met alle betrokkenen en de externe accountant.

Heeft het bestuur het oog nog op de bal?

De auditcommissie kan het bestuur ook vragen of er behoefte is aan meer ondersteuning, in de vorm van mensen en middelen. Een onderzoek kan het bestuur veel tijd en energie kosten, waardoor de dagelijkse aansturing van het bedrijf te weinig aandacht krijgt. De auditcommissie zal monitoren of de cfo en de rest van de bestuursleden het oog nog voldoende op de bal hebben.

Proactief naar buiten treden

Even belangrijk als het managen van de crisis is het managen van de communicatie met de belangrijkste stakeholders, zoals de medewerkers, de aandeelhouders en de kapitaalverstrekkers, klanten en leveranciers, externe toezichthouders, (sociale) media en het grote publiek. De auditcommissie kan het bestuur uitdagen om regelgevende instanties en externe toezichthouders uit eigen beweging op de hoogte te stellen en zou hierin een klankbordrol voor het bestuur moeten vervullen. Proactieve communicatie kan een rol spelen bij de disciplinaire maatregelen die de organisatie krijgt opgelegd. Juridisch advies is cruciaal bij de beslissing om zelf naar buiten te treden met misstanden en onregelmatigheden. Zeker wanneer het beursgenoteerde ondernemingen betreft.

Wat, wanneer en naar wie communiceren over het onderzoek naar misstanden en onregelmatigheden?

De auditcommissie ziet erop toe of de organisatie een protocol heeft voor interne en externe communicatie.

Best practices:

- Benoem een woordvoerder.
- Spreek met één stem: centraliseer en/of regisseer de communicatie.
- Voorkom dat medewerkers zelf naar buiten treden via sociale media of de pers en formuleer en deel kernboodschappen, Q&A's, et cetera.
- Informeer medewerkers eerst of op zijn minst gelijktijdig met de externe stakeholders (hou bij beursgenoteerde bedrijven rekening met de koersgevoeligheid van de informatie).
- Wees alert op extern klokkenluiden, lekken naar de pers of uitingen op sociale media.
- Wees proactief in plaats van reactief.
- Houd geen dingen achter, maar wees open. Voorkom dat belanghebbenden gaan speculeren.
- Zorg voor goede procescommunicatie: geef aan hoe lang het onderzoek duurt, wanneer de (tussentijdse) uitkomsten verwacht worden en als deze bekend zijn: welke maatregelen de organisatie neemt. Geef ook aan wanneer de organisatie niet kan communiceren, bijvoorbeeld omdat resultaten op zich laten wachten of omdat de zaak onder de rechter is.
- Geef aan hoe de auditcommissie en de raad van commissarissen hebben gehandeld tijdens de crisis en zich van hun taken hebben gekweten.
- Vervul een klankbordrol voor het bestuur op het gebied van transparantie over de crisis in het bestuursverslag, halfjaar- en eventuele kwartaalberichten en andere vormen van (financiële en niet-financiële) communicatie, zowel schriftelijk als mondeling.
- Besteed aandacht aan de crisis en het toezicht op het managen daarvan in het verslag van de auditcommissie (als onderdeel van het verslag van de raad van commissarissen in het jaarverslag).



7. Eindrapportage en het herstelplan

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Als het onderzoek naar misstanden en onregelmatigheden gereed is, worden de uitkomsten aan de auditcommissie gepresenteerd. De auditcommissie vergelijkt de eindrapportage met het oorspronkelijke plan van aanpak en kan daarbij de volgende vragen stellen:

- Hebben de onderzoekers de vooraf bepaalde scope daadwerkelijk gehanteerd en is deze voldoende breed en diepgaand gebleken? Of is niet of onvoldoende onderzocht of de misstanden en onregelmatigheden zich ook elders in de organisatie zouden kunnen voordoen?
- Is het onderzoek onafhankelijk en adequaat uitgevoerd?
- Wordt helder verslag gedaan van de bevindingen?
- Zijn de aanbevolen maatregelen afdoende om herhaling te voorkomen?

Herstelplan monitoren

Als de auditcommissie concludeert dat het onderzoek toereikend is en kan worden afgerond, is het nodig om een herstelplan op te stellen en uit te voeren: een plan van aanpak voor het omgaan met de gevolgen van de fraude of andere misstanden en onregelmatigheden en maatregelen om herhaling te voorkomen. Daarbij kan bijvoorbeeld gedacht worden aan ontslag van betrokken medewerkers, aangifte bij de betrokken instantie(s), het repareren van gevaarlijk zwakke plekken in de interne risicobeheersings- en controlesystemen en het corrigeren van de financiële verslaggeving. De auditcommissie zal de opstelling en uitvoering

van het herstelplan nauwgezet monitoren.

Wel of geen aangifte doen?

Organisaties zijn vaak terughoudend met het doen van aangifte van fraude of andere misstanden en onregelmatigheden. Dit kan echter publiekelijk overkomen als een poging tot ‘wegmoeffelen’ van het integriteitsprobleem. Het is verstandig vooraf beleid te bepalen of bij wetsovertredingen standaard aangifte wordt gedaan, of dat dit afhangt van de specifieke casus.

Afstemmen met de externe accountant over het onderzoek en het herstelplan

De auditcommissie zal voor het beoordelen van de uitkomsten van het verrichte onderzoek en het herstelplan afstemming zoeken met de externe accountant. Bij (het vermoeden van) fraude spreekt de externe accountant van tevoren af dat het bestuur, de raad van commissarissen of de auditcommissie de uitkomsten van het onderzoek en de te nemen maatregelen delen en de accountant inzage geven in het onderliggende dossier. Als de accountant het uitgevoerde onderzoek ontoereikend vindt, dan zal hij of zij aanvullend onderzoek verlangen om een controleverklaring te kunnen afgeven bij de voorliggende jaarrekening. Immers, als onzeker is of er (mogelijk) nog meer fouten in de cijfers hersteld moeten worden, dan kan de jaarrekening onjuist zijn. Ook kan het onzeker zijn of het bestuur integer is, waardoor de accountant mogelijk niet op de bevestiging van het bestuur bij de jaarrekening kan vertrouwen. Indien de organisatie het verzoek om aanvullend



Welke vragen stellen bij het herstelplan?

De auditcommissie monitort de uitvoering van het herstelplan. Belangrijke vragen die de auditcommissie daarbij aan het bestuur kan stellen:

- Wie was bij de misstanden en onregelmatigheden betrokken of wist ervan?
- Welke oorzaken liggen ten grondslag aan de misstanden en onregelmatigheden?
- Hoe weten we dat eenzelfde soort misstanden en onregelmatigheden zich niet eerder heeft voorgedaan of in andere delen van de organisatie speelt of heeft gespeeld (olievlekwerking)?
- Welke (nood)maatregelen worden genomen?
- Welke veranderingen in beleidsmaatregelen, procedures, interne controle, cultuur en toon aan de top zijn nodig om herhaling te voorkomen?
- Hoe kunnen eventuele materiële afwijkingen in de financiële en niet-financiële verslaggeving worden gecorrigeerd en gecommuniceerd?



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

1. Meldingen van misstanden en onregelmatigheden
2. Wanneer een onderzoek en door wie?
3. Het samenstellen van het onderzoeksteam
4. Bepalen scope en procedures van het onderzoek
5. De uitvoering van het onderzoek
6. Communiceren over de voortgang van het onderzoek
7. Eindrapportage en het herstelplan
8. Na de crisis: trek de lessen

9. Communicatie

onderzoek niet wil of kan honoreren, heeft dit mogelijk impact op de verstrekking van de controleverklaring. Als de externe accountant wegens (vermeende) fraude een niet-goedkeurende controleverklaring afgeeft (of verwacht dat te zullen doen), dan is deze verplicht om dat te melden aan de AFM.

Opdracht beëindigen of heroverwegen

De externe accountant geeft ook aan welke eisen minimaal gesteld worden aan het herstelplan, beoordeelt of de maatregelen toereikend zijn of dat er (ook) andere acties nodig zijn en controleert of het herstelplan in gang wordt gezet door het bestuur en/of de auditcommissie. Als het herstelplan ontoereikend is (of als de organisatie weigert om een aanwijzing van fraude – verder – te onderzoeken), dan meldt de externe accountant een fraude van materieel belang bij de desbetreffende opsporingsdienst (de Nationale Politie), als er sprake is van een wettelijke controle. Ook zal de externe accountant in dat soort situaties overwegen of de controleopdracht kan worden gecontinueerd of voortijdig beëindigd wordt. De accountant is verplicht om het tussentijds beëindigen van een wettelijke controleopdracht te melden bij de AFM. Ook als de fraude van niet-materieel belang is en het herstelplan wel toereikend is, zal de accountant standaard overwegen welke gevolgen de gesignaleerde integriteitsrisico's hebben voor de controleopdracht.

Aanpassen van de financiële verslaggeving

Als onregelmatigheden materieel effect blijken te hebben op de financiële verslaggeving en/of of de verslaggeving van voorgaande jaren, kan het nodig zijn om jaar- of kwartaalcijfers uit te stellen tot het onderzoek volledig is afgerond. Dat kan leiden tot een koersval (bij beursgenoteerde organisaties), schending van bankconvenanten en beperkte toegang tot de kapitaalmarkt. Zorgvuldige communicatie is geboden, om onnodige onzekerheid te voorkomen.

Direct en zorgvuldig informeren belanghebbenden

Tijdige en zorgvuldige communicatie over fouten in de verslaggeving is essentieel. Het publiceren van onvolledige en foutieve of misleidende cijfers, die later gecorrigeerd moeten worden, kunnen de geloofwaardigheid en de reputatie van de organisatie ondermijnen, aanleiding geven tot juridische procedures van (groepen) belanghebbenden en tot aanwijzingen van toezichthouders leiden. Als al gepubliceerde cijfers (inclusief die van voorgaande jaren) moeten worden aangepast, is de organisatie verplicht om direct de aandeelhouders en andere stakeholders te informeren. Aanpassing van de financiële verslaggeving – en de daarmee gepaard gaande onzekerheid – kan enige tijd in beslag nemen.



8. Na de crisis: trek de lessen

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
 - 1. Meldingen van misstanden en onregelmatigheden
 - 2. Wanneer een onderzoek en door wie?
 - 3. Het samenstellen van het onderzoeksteam
 - 4. Bepalen scope en procedures van het onderzoek
 - 5. De uitvoering van het onderzoek
 - 6. Communiceren over de voortgang van het onderzoek
 - 7. Eindrapportage en het herstelplan
 - 8. Na de crisis: trek de lessen
- 9. Communicatie

Als het stof is neergedaald van het onderzoek naar misstanden en onregelmatigheden, het herstelplan gedegen is uitgevoerd en de crisis succesvol is bezworen, is het tijd voor reflectie en evaluatie. Kijk terug naar de casus en trek de lessen: wat kan de auditcommissie beter of anders doen om in een volgende crisis effectiever te acteren?

‘Never waste a good crisis’

Winston Churchill zou het al hebben gezegd, refererend aan het momentum dat na de Tweede Wereldoorlog ontstond voor de oprichting van de Verenigde Naties: **‘Never let a good crisis go to waste.’** Een crisis is een kans om als auditcommissie het eigen functioneren te evalueren en te verbeteren en daarmee een volgende crisis te helpen voorkomen.





Communicatie over CSRD en ESG

Met bestuur, raad van commissarissen en stakeholders

09

9. Communicatie over CSRD en ESG

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis

9. Communicatie

1. Communiceren met het bestuur
 2. Communiceren met de raad van commissarissen
 3. Communiceren met de stakeholders
- Bijlagen

De auditcommissie vormt een verbindende schakel tussen het bestuur en de raad van commissarissen, Internal Audit en de externe accountant. Daarnaast legt de auditcommissie verantwoording af aan de stakeholders. Goede informatie, communicatie en transparantie bepalen de kracht van de interne en externe (rapportage)keten.

De auditcommissie heeft de taak om de oordeels- en besluitvorming van de raad van commissarissen voor te bereiden op het gebied van audit en **control**. Goede informatievoorziening en effectieve communicatie zijn cruciaal voor het uitvoeren van de taken en verantwoordelijkheden.

Daarbij gaat het allereerst om de wettelijke taken van de auditcommissie:

- het monitoren en waarborgen van de integriteit en kwaliteit van de financiële en duurzaamheidsverslaggeving;
- het monitoren van de effectiviteit van de interne risicobeheersings- en controlesystemen;
- het monitoren van de wettelijke controle van de (geconsolideerde) jaarrekening;
- het beoordelen van de onafhankelijkheid van de externe accountant; en
- het vaststellen van de procedure voor de selectie van de externe accountant of de accountantsorganisatie en de voordracht tot verlening van de opdracht tot het verrichten van de wettelijke controle en – indien het gaat om een OOB – selectie van, selectie van

de externe accountant door middel van een aanbestedingsprocedure.

Daarnaast houdt de auditcommissie volgens de Code toezicht op het bestuur ten aanzien van onder meer:

- de relatie met en de naleving van aanbevelingen en opvolging van opmerkingen van de interne auditor en de externe accountant;
- de financiering van de vennootschap; en
- het belastingbeleid van de vennootschap.

Ook niet-financiële verslaggeving

De taken en verantwoordelijkheden van de auditcommissie strekken zich ook uit tot het bestuursverslag. Dat bevat naast financiële ook niet-financiële prestatie-indicatoren, met inbegrip van milieu- en personeelsaangelegenheden (artikel 2:391 BW).

Grote OOB's, moeten volgens de CSRD in het jaarverslag ook niet-financiële informatie publiceren over milieu-, sociale en personeelsaangelegenheden, eerbiediging van



In dit hoofdstuk komen de volgende onderwerpen aan de orde:

1. Communiceren met het bestuur
2. Communiceren met de raad van commissarissen
3. Communiceren met de stakeholders: rapporteren in het jaarverslag (als onderdeel van het verslag van de raad van commissarissen)

mensenrechten, bestrijding van corruptie en omkoping. De auditcommissie moet ook de integriteit en kwaliteit van deze niet-financiële verslaggeving monitoren en waarborgen en de risico's op dit gebied bewaken. Tegenwoordig hebben steeds meer rvc's een separate commissie die gaat over duurzaamheid. Het is belangrijk om de taken met deze commissie, de auditcommissie en de gehele raad van commissarissen af te stemmen.

Informatievoorziening: halen en brengen

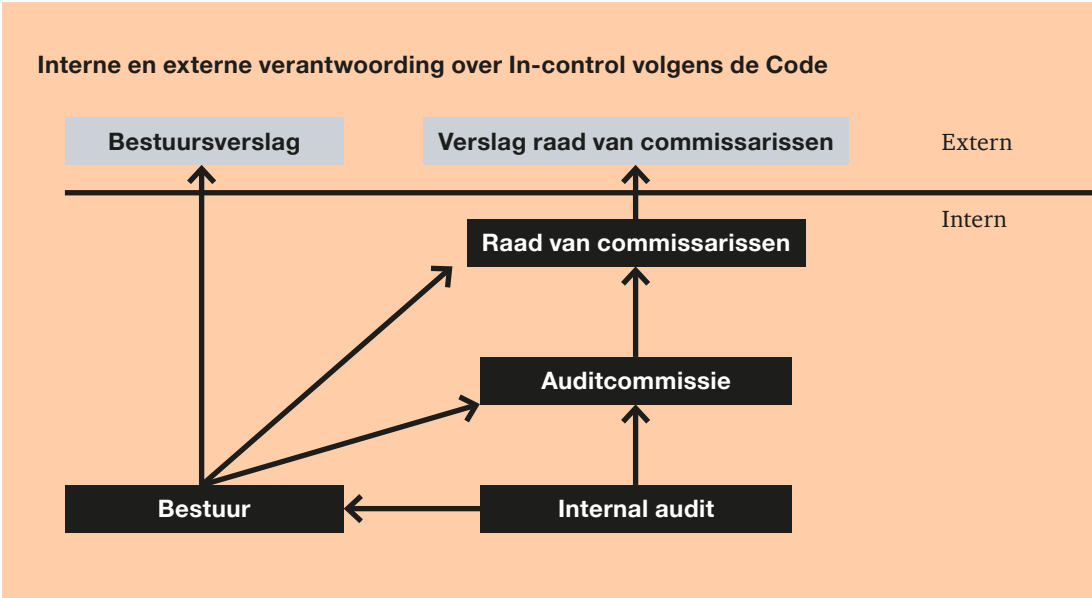
Het is van belang dat de auditcommissie voldoende zicht heeft op al deze toezichtthema's om haar taken goed te kunnen uitvoeren en daarover intern en extern verantwoording af te leggen. Op grond van artikel 2:141 BW heeft het bestuur de plicht om de raad van commissarissen tijdig de voor de uitoefening van diens taak noodzakelijke informatie te verschaffen, waaronder de hoofdlijnen van het

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholdersBijlagen

strategische beleid, de algemene en financiële risico's en het beheersings- en controlesysteem van de organisatie. De auditcommissie zal echter ook proactief op zoek gaan naar de gewenste informatie en intensieve contacten onderhouden binnen en buiten de onderneming: intern met het bestuur, het overige management en Internal Audit, extern met de accountant en de stakeholders, aan wie ook verantwoording wordt afgelegd (via het verslag van de raad van commissarissen). Daarnaast moet de auditcommissie de volledige raad van commissarissen goed informeren.

De auditcommissie heeft dus een haal- en brengplicht: de auditcommissie wordt geacht informatie te verstrekken, maar ook zelf actief informatie te vergaren.

De relatie met Internal Audit en de externe accountant komt hier slechts kort aan de orde en wordt in hoofdstuk 6 van deze publicatie uitgebreid besproken.



1. Communicatie met het bestuur

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholdersBijlagen

Het bestuur – en in het bijzonder de cfo – is de primaire informatiebron van de auditcommissie. Het bestuur bespreekt in elk geval de volgende zaken met de auditcommissie, volgens de Code:

- de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen (inclusief risicobeoordeling, implementatiesystemen en monitoring daarvan);
- belangrijke tekortkomingen in de interne risicobeheersings- en controlesystemen tijdens het boekjaar, plus eventuele significante wijzigingen of voorziene verbeteringen.

Gesprek aangaan over materiële risico's
Het gesprek tussen de auditcommissie en het bestuur over risicobeheersing en interne controle kent een brede scope. Zo benadrukt de Code expliciet dat de focus ligt op het gehele spectrum aan risico's:

- zowel intern als extern;
- zowel financieel als niet-financieel (op het gebied van strategie, naleving, bedrijfsvoering, IT (waaronder cyberrisico's), verslaggeving en cultuur (zoals de beloningsstructuur van bestuurders en werknemers).

Bovendien bespreekt en analyseert de auditcommissie volgens de Code ook de materiële risico's en onzekerheden die relevant zijn voor de continuïteit van de organisatie in de komende twaalf maanden. Het bestuur vermeldt die risico's en onzekerheden in het bestuursverslag en de VOR, de auditcommissie neemt de bevindingen van de eigen analyse op in haar verslag aan de

raad van commissarissen.

Daarnaast wisselt de auditcommissie in elk geval met het bestuur van gedachten over de eerdergenoemde thema's voor het toezicht op het bestuur, voortvloeiend uit de wet en de Code: de integriteit en kwaliteit van de financiële en duurzaamheidsverslaggeving, de wettelijke controle van de jaarrekening, de relatie met Internal Audit en de externe accountant, de financiering en het belastingbeleid. Verder kan de auditcommissie natuurlijk specifieke onderwerpen met het bestuur bespreken.

■ **De rol van de auditcommissie**

Zelf onderwerpen agenderen
Als het bestuur deze en andere onderwerpen niet uit eigen beweging ter bespreking voorlegt, kan de auditcommissie het initiatief naar zich toetrekken door onderwerpen **zél**f te agenderen. Denk bijvoorbeeld aan belangrijke investeringen, financiële prognoses en meerjarenprojecties, de planning-en-controlcyclus, significante schattingen in de jaarrekening en de actuele vraag hoe verantwoord de organisatie zich opstelt.

Achteraf of vooraf?
De auditcommissie kan ook aangeven wanneer ze (en daarmee dus de raad van commissarissen) geïnformeerd wil worden over welke soort beslissingen: pas achteraf of al vooraf? Dat hangt ook samen met de situatie of fase waarin

de organisatie zich bevindt: is er sprake van een stabiele of turbulente omgeving, zijn er grote veranderingen in de organisatie gaande (een strategische herstructurering, krimp of juist groei), is het financieel leiderschap wel of niet goed belegd? Het is de rol van de auditcommissie om het bestuur aan de voorkant van het besluitvormingsproces te adviseren bij fundamentele keuzes door te fungeren als klankbord. Vroegtijdige betrokkenheid maakt bovendien tijdig bijsturen mogelijk.

Robuuste dialoog
Goede communicatie kenmerkt zich door tweerichtingsverkeer: een robuuste dialoog tussen de auditcommissie en het bestuur. Als vooruitgeschoven post van de raad van commissarissen stelt een effectieve auditcommissie zich proactief op. Dat houdt in: het bestuur kritisch bevragen, maar ook dóórvragen als het antwoord onbevredigend is. Het gaat om **constructive challenge**: het bestuur op opbouwende wijze uitdagen door het stellen van kritische vragen om de kwaliteit van het besluitvormingsproces te toetsen. Zie de voorbeeldvragen op de volgende pagina.

Bepaal zelf inhoud boardpack
Goede communicatie begint met goede en betrouwbare informatie. Het bestuur verstrekt de auditcommissie juiste en volledige informatie. De auditcommissie doet er echter verstandig aan ook zelf aan te geven welke informatie wordt verlangd en zich ook daarin niet afwachtend op te stellen ten opzichte van het bestuur. Het bestuur

Best practice
Door onderwerpen simpelweg te agenderen, stimuleert de auditcommissie het bestuur erover na te denken en er een goede presentatie over te geven.

Een best practice is het hanteren van een jaaragenda waarin ten minste alle verplichte onderwerpen terugkomen, maar ook voor de organisatie belangrijke thema's aan bod komen. Daarbij is het gebruikelijk dat niet alleen bestuurders een presentatie verzorgen, maar ook functionarissen die verantwoordelijk zijn voor specifieke disciplines binnen de organisatie.

heeft immers niet alleen een brengplicht, de auditcommissie heeft ook een haalplicht. Voor de praktische ondersteuning kan daarbij de hulp van de bestuurssecretaris worden ingeroepen.

De eerder geschetste brede scope zorgt voor een grotere en andersoortige informatiebehoefte: naast financiële data, kpi's en **hard controls** moeten auditcommissies beschikken over niet-financiële, kwalitatieve informatie en **soft controls** in hun **boardpacks**. Zie bijlage 9A voor een overzicht van de onderwerpen waarover de auditcommissie in elk geval geïnformeerd wil worden.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis
9. Communicatie

1. Communiceren met het bestuur

2. Communiceren met de raad van commissarissen

3. Communiceren met de stakeholders

Bijlagen

Voorbeeldvragen voor een robuuste dialoog met het bestuur	
Welke vraag?	Wel of geen bevredigend antwoord?
Welke andere afwegingen hebben jullie gemaakt bij de totstandkoming van dit voorstel/dit besluit?	Heeft het bestuur inderdaad andere opties overwogen? Zijn er andere mogelijkheden die het management niet heeft meegenomen in de besluitvorming?
Welke alternatieven hebben jullie verworpen?	Zijn de redenen voor het verwerpen van alternatieven helder en begrijpelijk? Zijn ze gekoppeld aan het realiseren van een strategie?
Wat is jullie inschatting en beoordeling van de nadelen of risico's van deze beslissing?	Wordt er een compleet beeld geschetst?
	Komt de risicobeoordeling eerlijk en volledig over?
	Hoe worden de risico's gemitigeerd?
Wat doen onze concurrenten op dit gebied?	Zijn lessen uit het verleden meegenomen?
	Zijn de bedrijven die het bestuur aandraagt voor vergelijking de daadwerkelijke concurrenten op dit gebied?
	Is er bekeken of er disruptieve spelers zijn die de concurrenten van morgen kunnen zijn? Is er extern bewijs om de validiteit van het antwoord te ondersteunen?

Alternatieve informatiebronnen

De auditcommissie wil niet alleen afhankelijk zijn van de informatie die door het bestuur wordt verstrekt. Zowel de internal auditor als de externe accountant vormt een waardevolle aanvullende bron om de informatie van het bestuur in perspectief te kunnen zetten. Internal Audit en de externe accountant kunnen worden beschouwd als ‘bondgenoten’ van de auditcommissie. Ze houden immers eveneens toezicht op financiële verslaglegging, risicobeheer en interne processen. De auditcommissie beschikt over de rapportages van Internal Audit en de externe accountant en

onderhoudt daarnaast regelmatig contact met beide. Dat kan relevante inzichten opleveren.

Internal Audit als informatiebron

De auditcommissie kan vooraf zelf sturing geven aan de zaken waarover zij informatie en rapportages wenst te ontvangen van Internal Audit: door invloed uit te oefenen op het werkplan van Internal Audit, dat moet worden goedgekeurd door de raad van commissarissen. Het werkplan legt vast op welke wijze de auditcommissie door Internal Audit wordt geïnformeerd. Internal Audit heeft ook direct toegang tot de auditcommissie.

Bespreking van het werkplan biedt ruimte voor eigen vragen van de auditcommissie naar specifieke informatie of specifiek onderzoek. Bovendien bieden aparte contacten met bijvoorbeeld het hoofd Internal Audit gelegenheid voor het delen en toetsen van observaties.

Externe accountant als informatiebron

De auditcommissie kan ook invloed uitoefenen op de informatievoorziening door de externe accountant: via de reikwijdte en materialiteit van de controleopdracht en het controleplan, inclusief de belangrijkste risico's van de jaarverslaggeving die zijn benoemd in het controleplan. Ook hier biedt het bespreken van het controleplan en de bevindingen van de externe accountant – zoals neergelegd in de rapportage interim-bevindingen en het accountantsverslag – ruimte voor vragen van de auditcommissie. De auditcommissie overlegt zo vaak als nodig – maar ten minste één keer per jaar – buiten aanwezigheid van het bestuur met de externe accountant. Deze **private sessions** bieden bij uitstek gelegenheid voor het wederzijds delen van observaties ten aanzien van bijvoorbeeld de integriteit en kwaliteit van de verslaglegging en de robuustheid van risicobeheersing en interne controle (of het ontbreken daarvan).

Zoals eerder aangegeven: in hoofdstuk 6 wordt de relatie met Internal Audit en met de externe accountant uitgebreid besproken.

Andere interne en externe bronnen

Naast informatie van formele bronnen, kan de

auditcommissie zelf actief op zoek gaan naar informele bronnen, bijvoorbeeld door het oor te luisteren te leggen bij leden van het **executive committee**, de financiële kolom, de tax director en andere managers of stafffunctionarissen, of door hen uit te nodigen voor een presentatie tijdens de vergadering van de auditcommissie. Dit vindt plaats in overleg met het bestuur. Ook het bezoeken van een bedrijfsonderdeel of het bijwonen van een bedrijfsbijeenkomst als lid van de auditcommissie of als commissaris, kan relevante inzichten opleveren. Het geeft de auditcommissie meteen een inkijkje in de **soft controls**, de cultuur en de gehanteerde normen en waarden in de echelons onder de top. Daarbij is alertheid op waarschuwingssignalen geboden: signalen die kunnen duiden op integriteitsrisico's en/of ongewenst gedrag. (Zie voor voorbeelden hoofdstuk 4: Control & Compliance). Daarnaast kan zo nodig een beroep worden gedaan op externe adviseurs voor aanvullende informatie en expertise over specifieke thema's, of voor een second opinion.

De auditcommissie zal ook proactief op zoek gaan naar externe bronnen, als alternatief voor en aanvulling op de informatie van het bestuur. Het lezen van analistenrapporten, het bijhouden van de financiële pers en het volgen van de berichtgeving op internet en in de sociale media is onmisbaar voor een complete beeldvorming en zicht op de maatschappelijke context, onafhankelijk van het bestuur.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholdersBijlagen

Van toetsing achteraf naar toezicht op sturing
Proactief informatie vragen, zelf thema’s agenderen, het bestuur kritisch bevragen en de opvolging monitoren: de rolinvulling van de auditcommissie verschuift steeds meer van achteraf toetsen naar proactief toezicht op de totstandkoming van het beleid aan de voorkant van het strategische proces. Die actievere opstelling kan gemakkelijk leiden tot meer dynamiek tussen de raad van bestuur en de auditcommissie. Bestuurders kunnen het gevoel krijgen dat de auditcommissie op hun stoel gaat zitten. Dat geldt met name voor de cfo.

Van de voorzitter en de leden van de auditcommissie wordt dan ook rolvastheid verwacht: zoeken naar de juiste balans tussen actieve betrokkenheid bij het planning-en-controlproces en de gewenste afstand en onafhankelijkheid.

Best practice
Laat direct verantwoordelijke managers of staffunctionarissen een presentatie geven tijdens de vergadering van de auditcommissie. Bijvoorbeeld de cio als IT op de agenda staat. Observeer de dynamiek met het bestuur.

Durven doorvragen en uitdagen
Het bestuur wordt geacht zich op zijn beurt ‘open en aanspreekbaar’ op te stellen: het bestuur en de raad van commissarissen zijn volgens de Code elk verantwoordelijk voor het stimuleren van ‘openheid en aanspreekbaarheid’ binnen het eigen orgaan en de gremia onderling. Dat betekent wederzijds openstaan voor kritische vragen en tegenspraak. Dat geldt dus ook voor de auditcommissie. De voorzitter en de leden moeten net als de overige commissarissen beschikken over de onafhankelijkheid van geest voor een autonome oordeelsvorming, een kritische houding en de moed om het bestuur uit te dagen en door te vragen. Soms zal de auditcommissie – of een van de leden daarvan – de rol van advocaat van de duivel spelen. Dat pleit voor een divers samengestelde auditcommissie, die in de dynamiek met het bestuur verschillende rollen op zich kan nemen.

Vergaderen zonder ceo?
De cfo kan soms de behoefte hebben om zorgen te delen met de auditcommissie. Als het goed is, bestaat er een gezond spanningsveld tussen de cfo en de ceo. De cfo kan immers als rem fungeren voor de plannen van de ceo door op de financiële consequenties daarvan te wijzen. De auditcommissie zal de cfo graag de ruimte geven om zijn of haar visie te ventileren. Mede daarom is het best practice dat de ceo niet standaard aanwezig is bij de vergadering van de auditcommissie. De Code legt die beslissing bij de auditcommissie.

Alternatieve interne en externe informatiebronnen	
Intern	Extern
Wees op de hoogte van strategische besluiten en transformaties van het bedrijf en belangrijke businesstransacties door de tijd heen.	Volg de berichtgeving over het bedrijf in de media en op internet, inclusief de publieke opinie op fora en blogs.
Lees voorgaande jaarverslagen (in het bijzonder de discussie over de strategie en de risico’s).	Lees jaarverslagen, financiële berichten en niet-financiële informatie van de concurrentie.
Bezoek bedrijfsonderdelen, fabrieken en faciliteiten.	
Praat met marketing- en salesmanagers om inzicht te krijgen in producten en markten.	
Doorgrond de distributiekkanalen en weet wie de belangrijkste doelgroepen of klanten zijn.	
Doorgrond de supplychain en weet wie de belangrijkste leveranciers zijn.	
Weet wie de belangrijkste stakeholders zijn en wat hun belangen zijn.	Neem als toevoerder deel aan een dialoog van het bestuur met externe stakeholders.
Praat met managers en medewerkers van Finance, Tax en Treasury om de kapitaalstructuur, het belastingbeleid en de treasury-activiteiten te doorgronden.	Lees rapporten van ratingbureaus over de kredietstatus van het bedrijf.
Praat met Internal Audit.	Praat met de externe accountant.
Luister mee met calls van het management met analisten en de antwoorden op vragen van analisten.	Lees analistenrapporten over het bedrijf, de concurrenten en de sector.
Vraag het bestuur om inzage in correspondentie met en van de externe toezichthouder.	Ken de externe toezichthouders en hun agenda, plus de politieke en publieke druk waaronder deze opereren en de impact daarvan op het bedrijf, de manier waarop de toezichthouder de sector benadert en belangrijke issues voor het toezicht.

Spreek met de organisatie af hoe de auditcommissie toegang kan krijgen tot relevante informatiebronnen, of informatie aangeleverd wil krijgen.

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholdersBijlagen

Voorzitter auditcommissie belangrijk aanspreekpunt voor cfo

De ceo en cfo kunnen verschillende informele lijntjes hebben naar de raad van commissarissen, een logisch gevolg van ieders specifieke rol. De president-commissaris fungeert vaak als eerste aanspreekpunt voor de ceo, terwijl de cfo zich voor advies en bij dilemma's primair tot de voorzitter van de auditcommissie wendt, ook buiten de vergadering. Bij problemen met de ceo zal de cfo dan ook eerder contact opnemen met de voorzitter van de auditcommissie dan met de voorzitter van de raad van commissarissen. Het is belangrijk om de dynamiek tussen de ceo en cfo in goede banen te leiden om het ontstaan van twee kampen binnen en tussen het bestuur en de raad van commissarissen te vermijden.

Functioneren cfo beoordelen

Regelmatig contact met de cfo – zowel binnen als buiten de vergadering – heeft een bijkomend voordeel: het stelt de voorzitter, maar ook de andere leden van de auditcommissie, in staat om hem of haar te bevragen over de robuustheid van de financiële kolom en de kwaliteit van de bemensing. Bovendien kan de auditcommissie

Best practice

Wanneer het bestuur ontwijkende antwoorden geeft op vragen van de auditcommissie, of zich defensief opstelt, is dat te beschouwen als een waarschuwingssignaal op zichzelf.

zich door het een-op-een-contact een goed oordeel vormen over de capaciteiten en het functioneren van de cfo zelf en die informatie eventueel terugkoppelen naar de benoemings- en remuneratiecommissie voor de jaarlijkse evaluatie van de bestuursleden door de raad van commissarissen.



2. Communicatie met de raad van commissarissen

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis

- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholders
- Bijlagen

De auditcommissie is in het leven geroepen om de besluitvorming van de raad van commissarissen op het gebied van planning en control voor te bereiden. Het delegeren daarvan heeft belangrijke voordelen: de leden van de auditcommissie kunnen extra tijd besteden aan het doorgronden van de complexe financiële materie.

De auditcommissie heeft tijdens vergaderingen en daarbuiten rechtstreeks toegang tot de cfo, eventueel andere managers of staffunctionarissen, (het hoofd) Internal Audit en de externe accountant. Dat kan leiden tot meer verdieping en onafhankelijke informatie die de rapportage van het bestuur in perspectief zet en daarmee tot kritischer bevraging en verbetering van de besluitvorming van de gehele raad.

De auditcommissie zit ook als een spin in het web bij de benoeming en beoordeling van Internal Audit en de bespreking van het werkplan van deze afdeling. Hetzelfde geldt voor de benoeming van de externe accountant en het controleplan. De raad van commissarissen kan op basis van dit voorwerk sneller besluiten nemen over selectie, inzet en evaluatie van Internal Audit en de externe accountant.

Informatiekloof met raad van commissarissen dichten

De vooruitgeschoven positie van de auditcommissie kan wel zorgen voor een informatiekloof met de rest van de raad van de commissarissen. Om die kloof te dichten brengt de auditcommissie verslag uit aan de raad van



commissarissen. Het is een wettelijke taak van de auditcommissie om de raad van commissarissen (of het bestuur) in kennis te stellen van het resultaat van de wettelijke controle door de externe accountant, waarbij wordt toegelicht:

- op welke wijze de wettelijke controle heeft bijgedragen aan de integriteit van de financiële en duurzaamheidsverslaggeving, en;
- welke rol de auditcommissie in dat proces heeft gespeeld.

Ook de Code vereist dat de auditcommissie verslag doet aan de raad van commissarissen van haar beraadslaging en bevindingen.

In dat verslag komt in elk geval aan de orde:

- de manier waarop de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen is beoordeeld (inclusief risicobeoordeling, implementatie systemen en monitoring daarvan);
- de manier waarop de effectiviteit van het interne en externe auditproces is beoordeeld;
- de materiële overwegingen ten aanzien van de

financiële en duurzaamheidsverslaggeving; en

- de manier waarop de materiële risico's en onzekerheden zijn geanalyseerd en besproken en de belangrijkste bevindingen en de wijze waarop de verklaring omtrent risicobeheersing (VOR) van het bestuur is onderbouwd.. Aan bod komen minimaal de materiële risico's en onzekerheden die relevant zijn voor de verwachting ten aanzien van de continuïteit van de vennootschap voor een periode van twaalf maanden na opstelling van het bestuursverslag.

De auditcommissie doet verder verslag van andere

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholders
 - Bijlagen

relevante zaken die tijdens de vergadering, de aparte contacten met Internal Audit en de **private sessions** met de externe accountant ter tafel zijn geweest.

Verslag aan de raad van commissarissen bevat kernissues voor de besluitvorming

De manier van rapporteren door de auditcommissie, de frequentie daarvan en de mate van detail wordt in overleg met de gehele raad van commissarissen bepaald. Best practices zijn:

- De gehele raad van commissarissen krijgt alle stukken die de auditcommissie krijgt.
- De gehele raad van commissarissen heeft een staande uitnodiging om zelf de vergaderingen van de auditcommissie bij te wonen.
- De gehele raad van commissarissen krijgt het verslag/de notulen van de auditcommissie, voorafgaand aan de vergadering van de raad van commissarissen.
- De voorzitter van de auditcommissie brengt daarnaast mondeling verslag uit – inclusief zijn/haar indrukken – en vraagt de leden van de auditcommissie of hij/zij volledig is geweest.

Mondeling verslag door voorzitter

Als de vergadering van de auditcommissie direct voorafgaat aan de vergadering van de raad van commissarissen, zal de commissievoorzitter vaak mondeling verslag uitbrengen. Onderwerpen van het mondelinge verslag kunnen zijn:

- een samenvatting van de werkzaamheden in de voorgaande periode;

- een inhoudelijke terugkoppeling: wat waren de belangrijkste bevindingen?;
- aanbevelingen over kernissues die om besluitvorming door de gehele raad van commissarissen vragen.

Dynamiek tussen de auditcommissie en de overige commissarissen

Ondanks de verslaglegging kunnen de overige leden van de raad van commissarissen het

gevoel hebben op achterstand te staan: de auditcommissie heeft immers vaker en directer contact met de cfo, Internal Audit en de externe accountant en toegang tot sleutelinformatie. De auditcommissie moet zich dan ook goed realiseren dat de uiteindelijke besluitvorming thuishoort bij de raad van commissarissen en moet veel aandacht besteden aan rapportage en verantwoording.



Best practice

Betrek de rest van de raad van commissarissen erbij

Auditcommissies hebben soms het gevoel dat de rest van de raad van commissarissen achteroverleunt bij financiële- en duurzaamheidsverslaggeving en risicobeheer. 'Als de auditcommissie ernaar gekeken heeft, zal het wel goed zijn.' Voorkom deze houding door goed te communiceren naar de raad van commissarissen en deze er actief bij te betrekken.

De auditcommissie opereert dus niet op eigen houtje en trekt de besluitvorming niet naar zich toe, maar betreft de overige commissarissen daar voldoende bij.



3. Communicatie met stakeholders

- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis

- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholders
- Bijlagen

De auditcommissie brengt niet alleen intern verslag uit (aan de raad van commissarissen), maar ook extern: aan de stakeholders. Het verslag is onderdeel van het verslag van de raad van commissarissen in het jaarverslag. In het verslag komt volgens de Code in elk geval aan de orde:

- de samenstelling van de auditcommissie;
- het aantal vergaderingen (en de aanwezigheid daarbij van de auditcommissieleden);
- de belangrijkste onderwerpen die in de vergaderingen aan de orde zijn gekomen, inclusief de inhoudelijke toelichting daarop.

Verschil tussen intern en extern verslag
Opmerkelijk genoeg hanteert de Code slechts een algemene richtlijn voor het verslag van de auditcommissie, als onderdeel van het verslag van de raad van commissarissen. De Code geeft niet aan dat de auditcommissie extern moet rapporteren over dezelfde thema's als intern, namelijk in het verslag van de auditcommissie aan de raad van commissarissen, namelijk in het verslag van de auditcommissie aan de raad van commissarissen (zie pagina 63).

Tegemoetkomen aan roep om transparantie
Het ontbreken van de expliciete eis om extern over dezelfde zaken te rapporteren als aan de raad van commissarissen, geeft de auditcommissie juridisch gezien de ruimte om in het verslag van de raad van commissarissen niet in te gaan op een kernthema als bijvoorbeeld materiële risico's en onzekerheden voor de continuïteit. Voor stakeholders vormt dat juist belangrijke informatie. Hoewel de Code het dus

niet expliciet aangeeft, is het wel in de geest van de Code om transparant te zijn over het hart van de verantwoordelijkheid van de auditcommissie: toezicht houden op risicobeheersing, audit, financiële verslaglegging en continuïteit.

De auditcommissie komt daarmee bovendien tegemoet aan het maatschappelijke verwachtingspatroon en eventuele toekomstige regelgeving. De buitenwereld verwacht transparantie, ook van de auditcommissie. Zeker sinds de Code de rol van de auditcommissie heeft verzaamd. De auditcommissie die zich strikt tot de letter van de Code beperkt en in het externe verslag (als onderdeel van het verslag van de raad van commissarissen in het jaarverslag) niet ingaat op de vier punten waarover wel aan de raad van commissarissen wordt gerapporteerd, kan hier dan mogelijk ook vragen van aandeelhouders of andere stakeholders tegemoetzien.

Auditcommissies kunnen deze vragen voor zijn en de regie houden door in het externe verslag inhoudelijk in te gaan op voor stakeholders relevante thema's als risicobeheer en continuïteit: hoe heeft de auditcommissie deze thema's geanalyseerd en besproken en wat zijn de belangrijkste bevindingen?

Bestuursverslag en Verklaring van het bestuur¹

Het bestuur legt in het bestuursverslag verantwoording af over:

- (i) de uitvoering van de risicobeoordeling en de voornaamste risico's waarvoor de vennootschap zich geplaatst ziet in relatie tot haar risicobereidheid. Hierbij kan gedacht worden aan strategische, operationele, financiële, compliance en verslaggevingsrisico's;
- (ii) de opzet en werking van de interne risicobeheersings- en controlesystemen over het afgelopen boekjaar;
- (iii) eventuele belangrijke tekortkomingen in de interne risicobeheersings- en controlesystemen die in het boekjaar zijn geconstateerd, welke eventuele significante wijzigingen in die systemen zijn aangebracht, welke eventuele belangrijke verbeteringen van die systemen zijn voorzien en dat deze onderwerpen besproken zijn met de auditcommissie en de raad van commissarissen; en
- (iv) de gevoeligheid van de resultaten van de vennootschap voor materiële wijzigingen in externe omstandigheden.

Bestuursverklaring (responsibility statement):

Het bestuur verklaart in het bestuursverslag met een duidelijke onderbouwing dat:

- (i) het verslag in voldoende mate inzicht geeft in tekortkomingen in de werking van de interne risicobeheersings- en controlesystemen;
- (ii) voornoemde systemen een redelijke mate van zekerheid geven dat de financiële verslaggeving geen onjuistheden van materieel belang bevat;
- (iii) het naar de huidige stand van zaken gerechtvaardigd is dat de financiële verslaggeving is opgesteld op continuïteitsbasis; en
- (iv) in het verslag de materiële risico's en onzekerheden zijn vermeld die relevant zijn ter zake van de verwachting van de continuïteit van de vennootschap voor een periode van twaalf maanden na opstelling van het verslag.

¹ Geldend voor organisaties waarop de Nederlandse Corporate Governance Code van toepassing is.



1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

- 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholders
- Bijlagen

Spiegel van bestuursverslag

Een inhoudelijke verantwoording van de auditcommissie naar buiten maakt de cirkel ook mooi rond. Ook het bestuur moet namelijk inhoudelijk en onderbouwd verantwoording afleggen over risicobeheersing, de integriteit en kwaliteit van de financiële verslaglegging en de continuïteit: in het bestuursverslag in het jaarbericht en in de daarin opgenomen verklaring omtrent risicobeheer (VOR) van het bestuur. (van toepassing voor organisaties die onder de Code vallen, zie kader op voorgaande pagina). Als ook de auditcommissie in het eigen externe verslag (als onderdeel van het verslag van de raad van commissarissen in het jaarverslag) inhoudelijk op deze zaken ingaat en aangeeft hoe zij daarmee in het verslagjaar is omgegaan, is dat een logische aanvulling op het bestuursverslag en de bestuursverklaring. Zo ontstaat een compleet, helder en eenduidig beeld voor de stakeholders: de eigen medewerkers, aandeelhouders, eventueel de externe toezichthouders, de politiek, de media en de samenleving.

Transparantie over kritische issues en zorgen bij verslaggeving

Het zou logisch zijn als bij organisaties waarop de Code van toepassing is naast het bestuur ook de auditcommissie in het eigen verslag (als onderdeel van het verslag van de raad van commissarissen in het jaarverslag) materiële overwegingen bij de financiële- en duurzaamheidsverslaggeving (zoals majeure risico's en belangrijke schattingen) expliciet maakt. Het ligt in de rede te verwachten dat de materiële overwegingen/onzeakerheden die

de auditcommissie aanpakt ook de zogenoemde **key audit matters** raken, zoals die worden opgenomen door de externe accountant in de uitgebreide controleverklaring bij de jaarrekening (ook wel **long form opinion** of informatieve controleverklaring genoemd). **Key audit matters** zijn de belangrijkste aandachtspunten in de accountantscontrole volgens de externe accountant. Voorheen deelde de accountant kritische issues en eventuele zorgen bij de controle alleen intern. Sinds de invoering van de uitgebreide controleverklaring van de accountant in het jaarverslag (**long form opinion** of informatieve controleverklaring) bij OOB's, worden deze nu ook extern gerapporteerd en kunnen stakeholders er vragen over stellen. Sinds ook een groot aantal semipublieke organisaties¹ de status van OOB heeft gekregen, geven accountants bij deze organisaties eveneens een

uitgebreide controleverklaring in het jaarverslag. Voor private ondernemingen geldt deze verplichting (voorlopig nog) niet.

Reflecteren vanuit toezichtrol

Wanneer ook de auditcommissie extern rapporteert over de materiële overwegingen bij de jaarrekening en de andere kernthema's in de governance van de organisatie (zoals risicobeheer en continuïteit) – naast het bestuur en de externe accountant – is de cirkel rond: het bestuur rapporteert over belangrijke risico's in de risicoparagraaf en kritische schattingen en oordelen in de jaarrekening, de accountant geeft weer hoe hij of zij de belangrijkste zaken in de controle heeft aangepakt en de auditcommissie reflecteert op beide vanuit haar toezichtrol. De geboden transparantie kan bijdragen aan het herstel van maatschappelijk vertrouwen in de

Britse auditcommissie rapporteert over kritische overwegingen/onzeakerheden in de jaarrekening

Anders dan de Nederlandse Corporate Governance Code, verlangt de Britse code voor goed bestuur dat auditcommissies in een apart onderdeel van het jaarverslag inhoudelijk verslag doen over de belangrijkste kwesties in de financiële verslaglegging. De auditcommissie geeft in het verslag haar mening over 'de kwesties van betekenis inzake de financiële verklaringen' en hoe daarmee is omgegaan. Daarnaast gaat de auditcommissie in haar verslag in op de beoordeling van de effectiviteit van het externe controleproces, de gekozen benadering bij de (her)benoeming van de externe accountant, de zittingstermijn van de huidige accountant, de meest recente en aanstaande aanbestedingen en het waarborgen van objectiviteit en onafhankelijkheid bij eventuele dienstverlening buiten de controle.



¹ Sinds 1 januari 2020 hebben de aangewezen semipublieke instellingen, netbeheerders, grote woningbouwcorporaties, grote pensioenfondsen en drie instellingen voor het wetenschapsbeleid (KNAW, NWO en Koninklijke Bibliotheek), ook een OOB-status verkregen.

1. Commissie
2. Continuïteit
3. Corporate impact
4. Control & Compliance
5. Cultuur en gedrag
6. Checks & Balances
7. Corporate Reporting
8. Crisis

9. Communicatie

1. Communiceren met het bestuur
 2. Communiceren met de raad van commissarissen
 3. Communiceren met de stakeholders
- Bijlagen

integriteit van de verslaggeving en in de kwaliteit van het interne toezicht.

Hoe verslag doen over aandachtspunten en onzekerheden?

Zoals gezegd, vormen **key audit matters** – zoals gerapporteerd door de accountant – de belangrijkste aandachtspunten in de controle. Denk bijvoorbeeld aan significante schattingen (zie ook kader). De externe accountant benoemt deze aandachtspunten en plaatst deze in de specifieke context van de organisatie. Bij OOB's is de accountant verplicht deze aandachtspunten ook extern via zijn of haar controleverklaring te rapporteren.

In het verslag van de raad van commissarissen kan de auditcommissie voor de volgende opbouw kiezen bij het behandelen van de risico's en aandachtspunten:

- De auditcommissie ziet aandachtspunten en onzekerheden in de financiële en duurzaamheidsverslaggeving en benoemt deze.
- Deze aandachtspunten en onzekerheden komen overeen met de aandachtspunten die de externe accountant in de controleverklaring schetst.
- De auditcommissie heeft zich ervan vergewist dat het bestuur de door de auditcommissie gesignaleerde onzekerheden en de aandachtspunten van de externe accountant erkent.
- De auditcommissie heeft vastgesteld dat deze onzekerheden/aandachtspunten terugkomen in de interne risicobeoordelingen en de evaluatie van de interne risico-beheersings- en

controlesystemen en adequaat zijn toegelicht en verwerkt in de jaarrekening en het bestuursverslag.

Bij andere organisaties dan OOB's deelt de externe accountant de aandachtspunten bij de controle alleen intern, maar ook daar kan het benoemen van de **key audit matters** het startpunt vormen voor het mitigeren van de gesignaleerde verslaggevingsrisico's. Zie bijlage 9B voor een voorbeeldinhoudsopgave van het verslag van de auditcommissie in het jaarverslag als onderdeel van het verslag van de raad van commissarissen.

Transparant over rapportage interim-bevindingen en accountantsverslag?

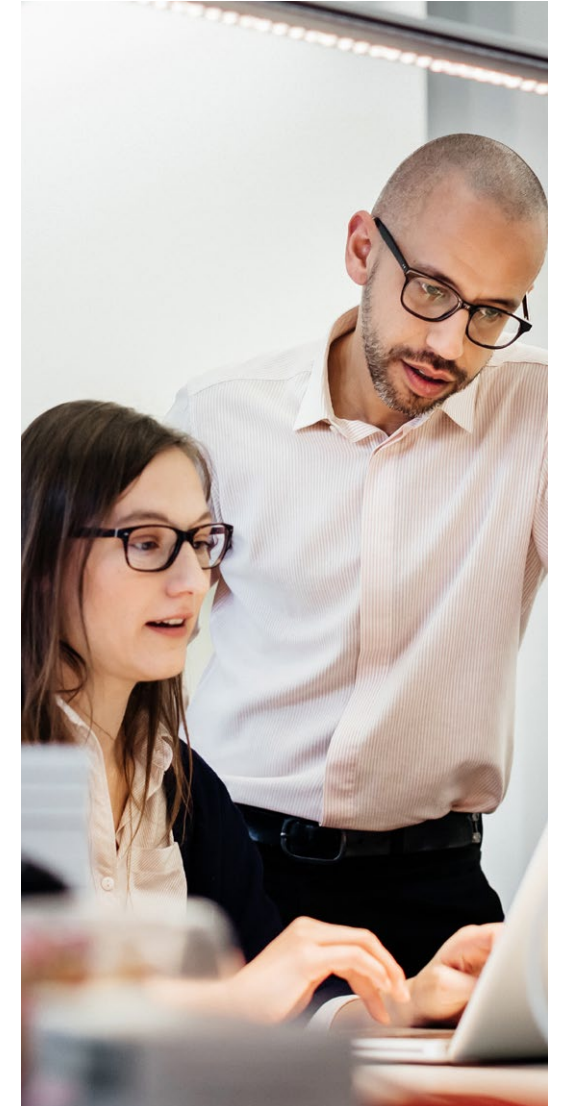
Een andere kwestie is openheid over de rapportage interim-bevindingen en het accountantsverslag en/of in het bestuursverslag. De rapportage interim-bevindingen en het accountantsverslag zijn niet geschreven als publieke rapportage, maar zijn primair bedoeld voor een open communicatie tussen de accountant, het bestuur en de commissarissen. Er is bij de stakeholders een blijvende roep om transparantie en om de inhoud van de rapportage interim-bevindingen en het accountantsverslag te publiceren.

Rapporteren over significante schattingen in verslag auditcommissie

Het doen van schattingen is inherent aan het opstellen van de jaarrekening. De externe accountant is alert op schattingen die een materiële impact kunnen hebben omdat ze een verhoogd risico met zich meebrengen en kan deze aanmerken als **key audit matter**. De auditcommissie kan in haar eigen verslag ingaan op welke significante schattingen zij identificeert en aangeven en hoe ze daarop toezicht heeft gehouden, en/of: welke vragen ze daarover aan het bestuur heeft gesteld.²

Openheid over schattingen bij niet-beursgenoteerde ondernemingen

In de jaarrekening moet informatie worden verstrekt over de significantie van schattingen. Als het bestuur niet transparant is over significante schattingen, zal de auditcommissie erop aandringen om deze informatie alsnog op te nemen in de jaarrekening en wijzen op het belang van openheid voor de organisatie en de stakeholders.



- 1. Commissie
- 2. Continuïteit
- 3. Corporate impact
- 4. Control & Compliance
- 5. Cultuur en gedrag
- 6. Checks & Balances
- 7. Corporate Reporting
- 8. Crisis
- 9. Communicatie
 - 1. Communiceren met het bestuur
 - 2. Communiceren met de raad van commissarissen
 - 3. Communiceren met de stakeholdersBijlagen

De auditcommissie/raad van commissarissen heeft inzage in de rapportage bevindingen én in de belangrijkste discussiepunten tussen de externe accountant en het bestuur naar aanleiding van de concepten van de rapportage interim-bevindingen en het accountantsverslag, aldus de Code. Voor het rapporteren van de bevindingen van de accountant door de auditcommissie in het externe verslag van de raad van commissarissen, gelden de volgende best practices:

- Zorg voor een evenwichtige weergave (niet te positief of negatief).
- Zorg dat stakeholders de boodschap van de accountant in de juiste context kunnen plaatsen zonder de volledige achtergrond te kennen.
- Maak de afweging of het verslag de beste plek is om deze transparantie te bieden of dat bijvoorbeeld het bestuursverslag of de aandeelhoudersvergadering een beter podium vormt.

Communicatie tijdens de aandeelhoudersvergadering
De algemene vergadering van aandeelhouders (ava) wordt geleid door de president-commissaris. De voorzitter van de auditcommissie is (net als de leden) standaard aanwezig bij de ava. Verwacht wordt dat de voorzitter van de auditcommissie vragen beantwoordt, onder meer over de benoeming en evaluatie van de externe accountant, maar bijvoorbeeld ook over de rapportage bevindingen en het accountantsverslag. Naarmate de auditcommissie zich transparanter opstelt in het eigen verslag (bijvoorbeeld over de **key audit matters**), zal

er bij stakeholders wellicht minder behoefte zijn aan toelichting door de voorzitter van de auditcommissie op de ava. Eventuele vragen worden immers al in het verslag van de auditcommissie beantwoord. Aan de andere kant kan die informatie ook vervolgvragen oproepen.

Stem voor ava goed af met de externe accountant

Best practice is dat de externe accountant tijdens de aandeelhoudersvergadering een korte toelichting geeft op de werkzaamheden en de uitgebreide controleverklaring, om vragen voor te zijn. Ook hier is een goede rolverdeling belangrijk:

- Stem als bestuur (ceo en cfo) en auditcommissie (voorzitter) vooraf de procedures en communicatie tijdens de ava af met de externe accountant.
- Vraag de toelichting van de externe accountant vooraf ter lezing.
- Bespreek welke onderwerpen mogelijk tijdens de ava aan bod komen.
- Bespreek het verstrekken van inlichtingen door de externe accountant over ‘andere informatie’ (onder meer het bestuursverslag en de verklaring omtrent risicobeheer (VOR), het verslag van de raad van commissarissen, de corporategovernanceverklaring en eventuele aanvullende **assurance**, bijvoorbeeld duurzaamheidsverslag, cultuuraudit, et cetera).
- Bedenk vooraf welke vragen stakeholders tijdens de ava zouden kunnen stellen over risicobeheersing en interne controle en wie welke vragen zal beantwoorden.

- Zorg voor een goede taakverdeling: wie zegt wat wanneer en waarover? De externe accountant kan alleen de vragen over de controleverklaring en de controle beantwoorden, alle andere vragen zijn voor het bestuur of de raad van commissarissen.
- Als de accountant van mening is dat het bestuur, de raad van commissarissen of de auditcommissie tijdens de ava een onjuiste voorstelling van zaken geven, dan kan hij of zij de voorzitter van de vergadering vragen de vergadering te schorsen om de gelegenheid te bieden voor correctie. Als het bestuur of de raad van commissarissen de gegeven informatie niet wil corrigeren, dan zal de accountant dat zelfstandig doen.



Bijlagen

Bijlage 9A	Waarover wil de auditcommissie in elk geval worden geïnformeerd?
Bijlage 9B	Voorbeeldinhoudsopgave van het verslag van de auditcommissie

Bijlage 9A Waarover wil de auditcommissie in elk geval worden geïnformeerd?

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

1. Communiseren met het bestuur

2. Communiseren met de raad van commissarissen

3. Communiseren met de stakeholders

Bijlagen

Strategie en businessplan • strategie en businessplan: haalbaarheid, implementatie en gerichtheid op duurzame langetermijnwaardecreatie: - inclusief budget en middellangetermijnplan; - financiering; - (hoe) worden stakeholdermanagement, duurzaamheid en kernwaarden geïntegreerd in cultuur en bedrijfsvoering?; - anticipeert het businessmodel op nieuwe technologie?; - de voortgang van de executie van de (nieuwe) strategie en/of cultuurverandering aan de hand van kpi's; medewerkerstevredenheidsonderzoeken, et cetera; • de financiering van de vennootschap; • de risicobereidheid; • (kwaliteit en betrouwbaarheid van de) managementinformatie. Maatschappelijke impact/ESG • (hoe) worden ESG-factoren (environment, social en governance) geïntegreerd in cultuur en bedrijfsvoering?; • personeelsbeleid, diversiteit en opvolgingsbeleid. Risicobeheersing • de materiële risico's (zowel financieel als niet-financieel) van de strategie, de activiteiten en de cultuur van de onderneming (zoals de beloningssystematiek), inclusief de gevoeligheid van de onderneming voor digitalisering en disruptie of andere veranderingen in de externe omgeving en reputatierisico's; • de toepassing van informatie- en communicatietechnologie door de vennootschap, waaronder risico's op het gebied van responsible AI en cybersecurity; en	• het belastingbeleid: - wat is de maatschappelijke visie en alignment met de kernwaarden?; - zijn we aantoonbaar in control: is het (internationale) raamwerk ingericht op het voorkomen, detecteren en beperken van problemen?; • fraude, corruptie en witwassen: de uitkomsten van het frauderisicoassessment, hoe vaak is het voorgekomen en hoe is daarmee omgegaan?; • de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen in de gehele organisatie: in hoeverre zijn deze geïntegreerd in de werkprocessen en bekend bij betrokken medewerkers?; • in hoeverre voldoen de interne risicobeheersings- en controlesystemen aan de algemeen geaccepteerde raamwerken (zoals het COSO-raamwerk)?; • tussentijdse uitkomsten van de monitoring van de werking van de interne risicobeheersings- en controlesystemen en de jaarlijkse systematische beoordeling daarvan: belangrijke tekortkomingen en doorgevoerde of voorziene verbeteringen; • geconstateerde zwaktes, misstanden en onregelmatigheden, signalen van klokkenluiders en geleerde lessen. Internal Audit • auditplan, (tussentijdse) bevindingen, aanbevelingen en opvolging van opmerkingen van de interne auditor en de naleving daarvan. Externe accountant • verantwoordelijkheden van de externe accountant met betrekking tot de controle van de financiële overzichten; • controleplan, inclusief een overzicht van de geplande reikwijdte en de timing van de controle (inclusief timing van de communicatie), de significante	risico's die door de externe accountant zijn geïdentificeerd, de materialiteit en de reikwijdte van de groepscontrole, voor zover van toepassing; • (tussentijdse) bevindingen, significante aangelegenheden die op grond van de professionele oordeelsvorming van de accountant relevant zijn voor het toezicht op het proces van (niet-) financiële en duurzaamheidsverslaggeving, uitkomst wettelijke controle, aanbevelingen en opvolging van opmerkingen van de externe accountant en de naleving daarvan; • (concept)rapportage interim-bevindingen en accountantsverslag; • de onafhankelijkheid van de externe accountant, met name de verlening van niet-assurancediensten aan de rechtspersoon; en • eventuele bevindingen van de toezichthouder over de kwaliteit van de uitgevoerde accountantscontrole. Verslaglegging • materiële overwegingen inzake de financiële- en duurzaamheidsverslaggeving?/integrated report, inclusief tussentijdse informatievoorziening als halfjaar- en kwartaalberichten en (earnings) conferencecalls met analisten; • materiële risico's en onzekerheden ten aanzien van de continuïteit van de vennootschap; • de wijze waarop de organisatie omgaat met nieuwe/ toekomstige verslaggevingsstandaarden; en • eventuele vragen van de toezichthouder over de financiële- en duurzaamheids-verslaggevingsstandaarden.
---	---	--



Bijlage 9B Voorbeeldinhoudsopgave van het verslag van de auditcommissie

1. Commissie

2. Continuïteit

3. Corporate impact

4. Control & Compliance

5. Cultuur en gedrag

6. Checks & Balances

7. Corporate Reporting

8. Crisis

9. Communicatie

1. Communiceren met het bestuur

2. Communiceren met de raad van commissarissen

3. Communiceren met de stakeholders

Bijlagen

Voorbeeld inhoudsopgave auditcommissie in het jaarverslag (als onderdeel van het verslag van de raad van commissarissen) 1. Samenstelling van de auditcommissie - leden en secretaris – namen en benoeming (eventueel korte biografische details); - bevestiging van het feit dat de leden van de auditcommissie voldoen aan de definitie van onafhankelijkheid (zoals voorgeschreven door de Code of andere regelgeving/organen); - benoemingsproces; 2. De rol van de auditcommissie - belangrijkste verantwoordelijkheden van de auditcommissie; - het reglement van de auditcommissie en eventuele aanpassingen, of een verwijzing naar de website; 3. Ondersteuning - de eventueel aan de auditcommissie beschikbaar gestelde menskracht (intern of ingehuurd); 4. Vergaderingen - de besproken onderwerpen (geen procesmatige beschrijving, maar inhoudelijke weergave): - audit en control op zowel financieel als niet-financieel gebied; - risicoprofiel strategie (businessplan versus financiering, bezien vanuit duurzame waardecreatie; - monitoring uitvoering strategie, eventuele cultuurverandering, et cetera;	5. Verslaggeving - beschrijving van de activiteiten die worden uitgevoerd om toezicht te houden op de integriteit van de verslaggeving; - bevestiging van het feit dat de auditcommissie de jaarrekening, het bestuursverslag en de onderbouwing van de verklaring omtrent risicobeheer (VOR) heeft besproken met het bestuur en de externe accountant; - materiële overwegingen bij de financiële en duurzaamheidsverslaggeving; - transparantie over relevante bevindingen van de accountant en visie op key audit matters en eventuele genomen of te nemen maatregelen; - eventueel: transparantie over de rapportage interim-bevindingen en het accountantsverslag; - duurzaamheidsrapportage of het integrated report en assurance daarover; - bevestiging van het feit dat de auditcommissie met de externe accountant eventuele andere kwesties heeft besproken zoals vereist door bepaalde wetten of regelgeving; - het belastingbeleid van de vennootschap; - de aanbeveling van de auditcommissie aan de raad van commissarissen over de goedkeuring van de gecontroleerde jaarrekening; 6. Risicobeheersing en interne controle - beschrijving van de beoordeling door de auditcommissie van de risicobeheersing van de onderneming in brede zin: analyse van interne en externe risico's (strategisch, operationeel, financieel, compliance, en verslaggeving); - implementatie van de interne risicobeheersings- en controlesystemen en monitoring daarvan, inclusief geconstateerde tekortkomingen, significante wijzigingen en voorziene verbeteringen; - de toepassing van informatie- en	communicatietechnologie door de vennootschap, risico's op het gebied van responsible AI; - materiële risico's en onzekerheden voor de continuïteit voor de komende twaalf maanden: hoe heeft de auditcommissie deze geanalyseerd en besproken en wat zijn de belangrijkste bevindingen? - geconstateerde zwakten, misstanden en onregelmatigheden, signalen van klokkenluiders, geleerde lessen en bevindingen van Internal Audit en de externe accountant: is daarmee rekening gehouden bij de risicobeoordeling?; 7. Internal Audit - beoordelingen uitgevoerd omtrent de plannen, het werk en de effectiviteit van de interne-auditfunctie; - kernresultaten in rapportage Internal Audit aan de auditcommissie: belangrijkste geconstateerde gebreken, bevindingen en observaties; - relatie van het bestuur met en de naleving van aanbevelingen en opvolging van opmerkingen van de interne auditor; - omschrijving van het toezicht van de auditcommissie op de interne-auditfunctie, of een beoordeling van de prestaties is uitgevoerd en wat daarvan de conclusies waren; - bij ontbreken Internal Audit: omschrijving van de auditcommissie waarom een dergelijke functie niet nodig is en welke adequate alternatieve maatregelen zijn getroffen. 8. Externe accountant - procedures ingesteld ter beoordeling van de onafhankelijkheid van de externe accountant, inclusief het beleid omtrent het verlenen van controle- en niet-controlediensten; - bevestiging van het feit dat de auditcommissie van de externe accountant een schriftelijke verklaring heeft ontvangen omtrent zijn of haar onafhankelijkheid,	en dat de onafhankelijkheid is besproken met de externe accountant en beoordeeld/bewaakt door de auditcommissie; - beschrijving van het toezicht van de auditcommissie op het externe controleproces en de effectiviteit daarvan; - relatie van het bestuur met en de naleving van aanbevelingen en opvolging van opmerkingen van de externe accountant; - bevestiging van het feit dat de prestaties van de externe accountant zijn beoordeeld en de uitkomsten daarvan; - de aanbeveling van de auditcommissie aan de raad van commissarissen voor de benoeming van de accountant en, indien van toepassing, het proces dat is ingesteld ter selectie van nieuwe accountants; - transparantie over gehanteerde selectiecriteria (inclusief materialiteit en scope) en inhoudelijke motivatie voor de voordracht: hoe en waarom is de auditcommissie tot de keuze gekomen?
--	---	---	--

Contactgegevens

Wilt u meer weten over de rol van de auditcommissie of andere governancethema's, neem dan contact op met:



Jacobina Brinkman
Managing Partner
Commissarissenontmoetingen
E: jacobina.brinkman@pwc.com

Met dank aan: Huub Wüst, Jos de Groot, Alexander Spek, Sander Kranenburg, Linda Thonen, Jan Driessen, Arjan Brouwer, Katja van der Kuij, Mona de Boer, Angeli Hoeksta, Wineke Ploos van Amstel-Haagsma, Marcus Looijenga

Deze publicatie vindt zijn oorsprong in het programma Commissarissenontmoetingen.
Kijk op www.pwc.nl/commissarissenontmoetingen voor meer informatie.

pwc.com

Bij PwC willen we een bijdrage leveren aan het vertrouwen in de maatschappij en het oplossen van belangrijke problemen. Wij zijn een netwerk van firma's in 149 landen met bijna 370.000 mensen. Wij zien het als onze taak om kwaliteit te leveren op het gebied van assurance-, belasting- en adviesdiensten. Bij PwC in Nederland werken ruim 5.900 mensen met elkaar samen. Vertel ons wat voor u belangrijk is. Meer informatie over ons vindt u op www.pwc.nl.

© 2025 PricewaterhouseCoopers B.V. (KvK 34180289) Alle rechten voorbehouden. PwC verwijst naar de Nederlandse firma en kan soms naar het PwC-netwerk verwijzen. Elke aangesloten firma is een afzonderlijke juridische entiteit. Kijk op www.pwc.com/structure voor meer informatie.