NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Monitoring Commissie Corporate Governance Code
Postbus 20401
2500 EK Den Haag

Per e-mail verzonden

Datum : 14 april 2022
Kenmerk : NOREA / AB22-29
Betreft : Consultatie actualisering Nederlandse Corporate Governance Code

Geachte Commissie,

Dank voor de geboden gelegenheid om te reageren op het voorstel voor actualisatie van de Nederlandse Corporate Governance Code (hierna Code).

Deze reactie versturen we als vertegenwoordigers van NOREA, de beroepsorganisatie van IT-auditors. Onze leden zijn nauw betrokken bij controles van jaarrekeningen en verstrekken rechtstreeks zekerheid en advies aan organisaties over informatietechnologie en informatiesystemen vaak gerelateerd aan de jaarrekening.

Wij onderschrijven de noodzaak om een effectieve en efficiënte Code te hebben voor hoogwaardige bedrijfsrapportage door (beursgenoteerde) ondernemingen en om ervoor te zorgen dat ondernemingen informatie eenduidig rapporteren die relevant is voor stakeholders.

In ons werkveld zien we dat als IT onvoldoende beheerst wordt door ondernemingen, dit leidt tot materiële risico's voor de onderneming die in enkele gevallen ook de continuïteit van de onderneming raken (denk o.a. aan cyberrisico's en outsourcingsrisico's). Meer en meer schrijft de accountant (lees NBA en NOREA) dan ook risico's inzake de beheersing van IT als Key Audit Matter (KAM) in de accountantsverklaring bij de jaarrekening. In het jaarverslag wordt hierover echter maar sporadisch melding gemaakt. Dit is temeer een reden om in de Code expliciet naar de risico's en de beheersing van IT en Cyber te verwijzen.

POSTADRES
POSTBUS 7984
1008 AD AMSTERDAM

BEZOEKADRES
ANTONIO VIVALDISTRAAT 2-8
1083 HP AMSTERDAM

E-MAIL EN WEBSITE
NOREA@NOREA.NL
WWW.NOREA.NL

OVERIG
TEL: 00 31 (0)20 301 03 80
KVK-NR: 40537540
IBAN: NL02ABNA0475165403

In onze reactie, zie bijlage bij deze brief, hebben we een aantal ontwikkelingen opgenomen uit ons vakgebied en geven enkele overwegingen aan u mee om de Code daarmee te verrijken.

De opbouw in onze reactie is als volgt:

1. Ontwikkelingen binnen ons vakgebied in relatie tot IT-beheersing (inclusief continuïteit) en de lange termijn waardecreatie van ondernemingen;
2. De nieuwe Code in relatie tot de ontwikkelingen;
3. Voorstel tot verrijking van de Code.

Onze reactie kan tevens gepubliceerd worden. Indien gewenst geven wij graag een nadere (mondelinge) toelichting op deze brief.

Met vriendelijke groet,

Namens het NOREA-bestuur,
Irene Vettewinkel-Raymakers RE,
Voorzitter

Bijlage bij brief d.d. 14 april 2022 met kenmerk NOREA / AB22-29

1. Ontwikkelingen

Binnen ons vakgebied zien we een aantal ontwikkelingen welke belangrijk zijn voor de lange termijn waardecreatie en de continuïteit van ondernemingen. We hebben "Ethics Washing" als voorbeeld verder uitgewerkt.

Belangrijke ontwikkelingen welke door ons worden gesignaleerd:

i. Nieuwe technologieën: Diensten en producten van onderneming worden steeds verder gedigitaliseerd daarbij gebruik makende van nieuwe technologieën. Deze digitale transformatie samen met nieuwe (EU-)regelgeving zullen gevolgen hebben voor de huidige en toekomstige ecosystemen en de wijze waarop daarover verantwoording wordt afgelegd. Voorbeelden zijn Internet of Everything, CSRD (o.a. niet-financiële rapportage), DORA & NIS2, blockchain-enabled smartcontracts, ESEF/XBRL, ESAP, realtime rapportage, nieuwe digitale economie met datagedreven financiering en het realiseren van 'verlicht aandeelhouderschap'.

ii. Toenemende cyberdreiging: De afgelopen jaren hebben grote (beursgenoteerde) bedrijven, die te maken hebben gehad met IT/cyber-gerelateerde incidenten, geleerd dat de continuïteit van de bedrijfsvoering afhankelijk is van betrouwbaar werkende IT-systemen. Zij begrijpen dat IT-systemen betrouwbaar moeten zijn ter ondersteuning van (financiële) (rapportage)processen. Het vermogen om aanvallen te detecteren of op incidenten te reageren hangt af van de wijze waarop deze bedrijven hun informatie- en communicatietechnologie beheersen (acquireren, beheren, onderhouden, controleren en uitfaseren).

iii. Toenemende ketenafhankelijkheid: We zien dat de levering van diensten en producten steeds vaker tot stand komt door samenwerking van verschillende ondernemingen. Dit deels door uitbesteding van specifieke activiteiten of door samenwerking tussen ondernemingen om te komen tot een eindproduct in de productieketen (of dienst). De afhankelijkheid van de ketenpartijen en geoutsourcete activiteiten, al dan niet met cloud, wordt essentieel voor de levering van producten en diensten. Maatschappelijk kijken we niet meer enkel naar een onderneming in de keten. De verantwoordelijkheid van een onderneming gaat over het aantoonbaar in control zijn en blijven over de uitbestede activiteiten en

maatschappelijk gezien ook steeds meer over het eindproduct in de productie- en waardeketen. Dit komt ook terug in de EBA Guidelines on outsourcing arrangements en het toenemende belang van Third-Party Risk Management.

iv. Data: De toenemende impact van data op onze levens en de transitie van besluitvorming door mensen naar meer besluitvorming gebaseerd op algoritmes brengt een breed scala aan nieuwe ethische (Ethical Washing) en privacy gerelateerde uitdagingen en dilemma's met zich mee. Denk hierbij aan de Ethische Richtsnoeren voor Betrouwbare Kunstmatige Intelligentie van de Europese Commissie. Een voorbeeld van Ethical Washing is hieronder weergegeven.

Ethics Washing

Om het belang op technologische ontwikkelingen voor het bestuur en de raad van commissarissen van Nederlandse beursvennootschappen te duiden, signaleren we een risico op "Ethics Washing" via technologie.

De hoeveelheden data die organisaties produceren en verzamelen, nemen exponentieel toe. Steeds meer organisaties ontsluiten de 'schatten' die in die data verborgen liggen. Of doen een poging hiertoe. Data-analyse levert kostbare inzichten op, waarmee bedrijven hun klanten beter kunnen bedienen, accuratere voorspellingen kunnen doen, risico's beter kunnen beheersen, de kans op fraude kunnen verkleinen en nieuwe patronen kunnen ontdekken die een voedingsbodem zijn voor nieuwe businessmodellen.
De analyse van grote hoeveelheden data is al lang geen handwerk meer. Voor geavanceerde data-analyse zijn organisaties aangewezen op automatisering. Algoritmes nemen de analyse over. Artificial intelligence (AI) en machine learning helpen om analyses voortdurend te verbeteren en inzichten steeds effectiever toe te spitsen op de grootst mogelijke waarde voor de business (Auditmagazine 21 juni 2021, vertrouwen in AI, Roelfsema, Krol & Renkema).

De inrichting van de technologie (bijv. AI) dient overeen te komen met de ethiek, cultuur en waarden van een organisatie. Het risico op "Ethics Washing" kan ontstaan als de technologische inrichting niet overeenkomt met de ethische waarden van een organisatie. Een gevolg kan zijn dat het consumentenvertrouwen daalt of dat zelfs reputatieschade geleden wordt, wat de continuïteit van een onderneming kan raken.

Als bestuur en raad van commissarissen wordt zorggedragen dat de ondernemingswaarden bijdragen aan de lange termijn waardecreatie. Het bestuur stimuleert het gedrag dat aansluit bij de ondernemingswaarden bij de medewerkers, de verbonden ondernemingen en ook via technologieën zoals AI. In dit verband is het dan ook van belang dat het bestuur of raad van commissarissen zichzelf de volgende vraag stelt:

Welke acties heeft u als bestuur of raad van commissarissen uitgezet om te komen tot betrouwbaar en ethisch verantwoord gedrag van technologische oplossingen zoals AI?

2. Actualisatie voorstel van de Code in relatie tot de ontwikkelingen

Graag leggen we op basis van bovenstaande ontwikkelingen de relatie met de nieuwe Code.

In Code zien we op pagina 12 bij de toelichting op Principe 1.1. "Lange Termijn Waardecreatie" dat *lange termijn waardecreatie verlangt van bestuurders en commissarissen bewustzijn van en anticiperen op ontwikkelingen in nieuwe technologieën en veranderingen in business modellen*.

Bij Principe 1.5.1. op pagina 36 staan de "Taken en verantwoordelijkheden van de auditcommissie" beschreven. *Zij richt zich onder meer op toezicht op het bestuur ten aanzien van: iii. de toepassing van informatie- en communicatietechnologie door de vennootschap, waaronder risico's op het gebied van cybersecurity*;

In de "Toelichting op enkele principes en best practice bepalingen" op pagina 63 staat in Principe 2.1.4. "Deskundigheid" dat: *Van belang is dat in het bestuur en de raad van commissarissen ook voldoende deskundigheid aanwezig is om tijdig kansen en risico's te signaleren die gepaard kunnen gaan met vernieuwingen in business modellen en technologieën*.

Het valt ons op dat ook in het voorstel van actualisatie slechts beperkt aandacht is voor informatietechnologie en cybersecurity.

3. Voorstel tot verrijking van de Code

Wij zijn van mening dat alignment tussen de Code en bovengenoemde trends en gerelateerde rapportagevereisten wenselijk is, met name voor grote organisaties met vaak complexe en uitgebreide (en vaak hybride cloud-enabled) IT-omgevingen en die door omvang en verwevenheid een grote maatschappelijke relevantie hebben.

Belanghebbenden tonen steeds meer interesse in de wijze waarop organisaties hun vitale IT en cyberveerkracht beheren en hoe ze ervoor zorgen dat de huidige en toekomstige Informatie – en communicatietechnologie de bedrijfsstrategieën op korte, middellange en lange termijn ondersteunen. Daarnaast dienen organisaties te zorgen voor de betrouwbaarheid in de productie-en waardeketen en zich bewust te zijn van hun maatschappelijke relevantie.

We adviseren om onderstaande principes te verrijken.

Principe 1.2 Risicobeheersing
We adviseren om in de risicobeheersing specifieke aandacht te besteden aan risico's op het gebied van cybersecurity, business continuity management, data governance & ethics, outsourcing, Digital Innovation & Transformation en privacy.

Principe 1.4.2. Verantwoording in het bestuursverslag
We adviseren om bij "*Hierbij kan gedacht worden aan strategische, operationele, compliance en verslaggevingsrisico's"* ook specifiek toe te voegen risico's op het gebied van de informatie- en communicatietechnologie.

Principe 1.4.3. Verklaring van het bestuur
Wij adviseren om hier toe te voegen aan de verklaring van het bestuur dat:

- Het verslag in voldoende mate inzicht geeft in tekortkomingen of incidenten in de informatie- en communicatietechnologie waaronder cyberweerbaarheid, data ethiek en privacy (datalekken) alsook in services welke van third parties worden afgenomen of zijn uitbesteed;
- Het verslag in voldoende mate inzicht geeft in de risico's en onzekerheden ten aanzien van de informatie- en communicatietechnologie voor een periode van 12 maanden na opstelling van het verslag.

Principe 1.5.1. Taken en verantwoordelijkheden auditcommissie
Wij adviseren om bij de zin "*iii. de toepassing van informatie- en communicatietechnologie door de vennootschap, waaronder risico's op het gebied van cybersecurity"* de volgende onderdelen toe voegen namelijk business continuity management, data governance & ethics, outsourcing, Digital Innovation & Transformation en privacy.

Mocht u in de Code de verantwoordelijkheden voor het bestuur en raad van commissarissen in algemene termen willen houden, wat we deels kunnen begrijpen vanwege de vele governance onderwerpen, dan adviseren we om één aanvulling wel op te nemen in Principe 1.5.3. Verslag auditcommissie.
De auditcommissie brengt verslag uit aan de raad van commissarissen over de beraadslaging en bevindingen. In dit verslag wordt in ieder geval vermeld:
Hier willen we aan toevoegen item V.:
V. De materiële risico's en de beheersing op Cybersecurity, Business Continuity Management, Data Governance & Ethics, Outsourcing, Digital Innovation & Transformation en Privacy.