

11 | Wat het zwaarste is, moet het zwaarste wegen: toezicht op organisatiecultuur praktisch benaderd vanuit risicoperspectief

Steven Brassem

1. Inleiding: de uitdaging

Het behoeft waarschijnlijk geen betoog dat de cultuur van een organisatie een belangrijke factor kan zijn voor haar succes. Over de hele wereld hebben wetenschappers dan ook onderzoek gedaan naar organisatiecultuur, getuige de indrukwekkende hoeveelheid literatuur die er op dit gebied te vinden is. Breed gedragen is intussen de ‘culture-eats-strategy-for-breakfast’-gedachte, oftewel: cultuur is – méér dan een ‘belangrijke factor’ – zelfs grotendeels bepalend.

Zo zijn er inderdaad voorbeelden van ondernemingen die hun spectaculaire groei in het bijzonder te danken hebben aan een cultuur gekenmerkt door innovatiedrang en snelle aanpassing (denk aan ‘big tech’). Daartegenover staan talloze gevallen in binnen- en buitenland van publieke en private organisaties waar het in de cultuur juist mis is gegaan, met reputatieschade, waardeverlies, en soms zelfs teloorgang tot gevolg. Het gaat dan meestal om kwesties op ethisch gebied, duurzaamheid, of gevallen van (structurele) misdragingen: soms rechtstreeks in of vanuit de top, maar vaak genoeg ook als gevolg van passiviteit of falend ingrijpen van het bestuur en de toezichthouders.

Het centrale belang van organisatiecultuur is inmiddels óók onderkend door de Monitoring Commissie Corporate Governance Code (hierna: de Commissie, en: de Code), door in de (in december 2022) aangepaste versie van de Code specifiek de verantwoordelijkheden van bestuur en toezichthouders ten aanzien van cultuur te definiëren. Principe 2.5 luidt: ‘Het bestuur is verantwoordelijk voor het vormgeven van een cultuur die is gericht op duurzame lange termijn waardecreatie van de vennootschap en de met haar verbonden onderneming. De raad van commissarissen houdt toezicht op de activiteiten van het bestuur ter zake.’ Dat de Code zo expliciet het doel van de organisatiecultuur benadrukt – duurzame langetermijnwaardecreatie – is interessant en ook welkom. Hierover meer later.

De Code verlangt voorts dat het bestuur in haar verslag een toelichting geeft op cultuurgerelateerde aspecten en hoe zij deze beoordeelt. Het bestuursverslag valt

op zijn beurt binnen de algemene scope van toezicht¹ door de RvC,² hetgeen als ‘double-dip’ oplevert dat zowel toezicht wordt gevraagd op hoe het bestuur met cultuur omgaat als op hoe zij hierover verantwoording aflegt. Het is overigens denkbaar dat onder omstandigheden de RvC zelf in haar eigen verslag een paragraaf besteedt aan dit onderwerp: een extra ‘dip’.

Er ligt dus een formidabele uitdaging voor zowel bestuurders als toezichthouders, die misschien inhoudelijk niet zozeer nieuw is maar nu in de Code is ‘gevangen’ met als gevolg ‘upped stakes’ en zwaardere rapportagevereisten. Het bereiken oftewel ‘vormgeven van een cultuur gericht op duurzame langetermijnwaardecreatie’ – en daar verantwoording over afleggen – kan al ingewikkeld genoeg zijn: de opdracht om daar effectief toezicht op te houden is dat zeker. De Code biedt echter geen handreiking in de vorm van in de praktijk te hanteren richtlijnen, en met name ten aanzien van toezicht zouden deze nu juist van nut kunnen zijn.

Om de taak in deze voor de RvC – in nauw overleg met het bestuur – meer hanteerbaar te maken kan een eenvoudige, procesgerichte benaderingswijze vanuit de te onderkennen relatie tussen cultuur en risico houvast bieden. Adequate aandacht voor risicomanagement vloeit immers ook al op natuurlijke wijze voort uit goede corporate governance, zoals de Code bedoelt te bewerkstelligen. Zo’n procesgerichte benaderingswijze vanuit het risicoperspectief kan er dan als volgt uitzien:

1. Vaststellen prioriteiten: welke strategische en tactische doelstellingen zijn (op dit moment) het meest belangrijk?
2. Aansluiten kernwaarden: welke culturele waarden zijn essentieel in relatie tot de vastgestelde prioriteiten?
3. Evalueren risicofactoren: welke risicofactoren en omstandigheden zijn er te onderkennen die van invloed kunnen zijn op het handhaven van de kernwaarden?
4. Taxeren risico’s: hoe groot zijn de risico’s dat de organisatiecultuur het bereiken van de belangrijkste doelstellingen in de weg staat?
5. Concluderen en handelen: is de informatie voldoende voor de RvC om tot een oordeel te komen en/of zijn er acties gewenst, zoals bijsturing of het verkrijgen van meer informatie en eventuele ‘assurance’?

In dit hoofdstuk zal ik deze voorgestelde vijf stappen afzonderlijk uitwerken. Eerst echter is het nodig om de twee centraal staande begrippen af te bakenen: organisatiecultuur en risico(management). Dit is belangrijk om het vervolg en het voorgestelde proces te begrijpen, terwijl nu juist beide begrippen weliswaar in de praktijk veel gebezigd toch niet altijd in al hun respectievelijke facetten volledig worden begrepen.

¹ Principe 1.5 van de Code stelt dat de integriteit en kwaliteit van de financiële- en duurzaamheidsverslaggeving onder het toezicht valt van de RvC.

² In navolging van de Code en om de leesbaarheid te bevorderen wordt hierna geen onderscheid gemaakt tussen een Raad van Commissarissen en een Raad van Toezicht en refereert de afkorting RvC aan beide.

2. Wat is organisatiecultuur en wanneer is deze effectief?

2.1 Cultuur

Ondanks de algemene consensus over de sleutelrol van cultuur in de onderneming, blijft het een lastig te doorgronden concept dat zich in de praktijk niet eenvoudig laat kennen, vatten, en (be)sturen. De Commissie geeft weliswaar een omschrijving in de toelichting op Principe 2.5 maar stelt daarbij: 'De Code adresseert cultuur, maar schrijft niet voor wat cultuur precies is of zou moeten zijn. Het is aan het bestuur om invulling aan cultuur te geven.' Vervolgens wijst zij er – terecht – op dat cultuur niet slechts als 'mono' is te bezien: 'Bij het vormgeven van cultuur wordt rekening gehouden met het bestaan van verschillende subculturen binnen de onderneming.'

Logischerwijze treedt culturele diversiteit in toenemende mate op naarmate de organisatie groter en complexer is. Verschillen kunnen zich voordoen tussen de bestuurskamer en de spreekwoordelijke werkvloer, tussen en binnen afdelingen, business units en werkmaatschappijen, en zeker ook in regionaal en internationaal opzicht. Voorts tussen beroepsgroepen of bij verschillende professionals. Terzijde valt daarbij op te merken dat culturele diversiteit ook voordelen kan opleveren. Het kan zelfs als kracht werken, zeker als culturele verschillen binnen de organisatie effectief worden overbrugd en dilemma's worden verenigd. Trompenaars en Hampden-Turner³ spreken in dit verband van 'cultural competence'. Aan de hand van een door hen ontwikkeld zevendimensionaal model om culturele verschillen, zoals die zich vooral op zogenaamd macroniveau kunnen voordoen (bijvoorbeeld nationaal, etnisch, geloofsovertuiging), worden deze inzichtelijk en in de praktijk hanteerbaar gemaakt. Cultuur op macroniveau is zeker ook van invloed op organisatiecultuur, waarbinnen dikwijls diverse subculturen zijn te onderscheiden en zelfs 'microculturen'.

Volgens het veel gebruikte model van Schein⁴ wordt cultuur voorgesteld als bestaande uit meerdere gelaagdheden, zoals die van een ui. De buitenste, waarneembare laag van deze ui is de expliciete uitdrukking van cultuur als zichtbare structuren, processen en gedragingen ('artefacts') en producten ('products'). Hieraan liggen op een dieper niveau gedeelde normen en waarden ten grondslag, die op hun beurt weer zijn gebaseerd op nog dieper gelegen fundamentele veronderstellingen in het onderbewuste (vanwaaruit bepaalde percepties, gedachten en gevoelens voortkomen). Een iets andere insteek (ook aangereikt door Schein) is om cultuur te omschrijven als de wijze waarop (groepen) mensen gewend zijn om gezamenlijk bepaalde soorten problemen op te lossen in de door ervaring ontstane overtuiging dat dit de juiste benaderingswijze is.

3 C. Hampden-Turner & F. Trompenaars, *Riding the Waves of Culture: Understanding diversity in global business*, UK: Nicholas Brealy Publishing 2012.

4 E.H. Schein, *Organizational Culture and Leadership*, USA, San Francisco (CA): Jossey-Bass 1985, 2004.

Een eveneens vaak gehanteerde metafoor is die van de ijsberg: het grootste en zwaarste deel ligt verscholen onder het wateroppervlak. DNB⁵ bedient zich van zo'n ijsberg-model bij het onderzoeken en beoordelen van cultuuraspecten binnen de financiële instellingen die onder haar externe toezicht vallen. Daarmee is veel ervaring opgedaan. Volgens het model dat DNB daarvoor heeft ontwikkeld – overigens wederom gebaseerd op Schein – is gedrag ('behaviours') de waarneembare manifestatie van cultuur, die zijn oorsprong vindt in onderliggende 'group dynamics', die op hun beurt weer zijn gebaseerd op de gedeelde 'mindset' (te weten de veronderstellingen en diepe overtuigingen in het onderbewuste van waaruit de werkelijkheid wordt begrepen). De DNB-benadering baseert zich erop dat uit waarneembaar gedrag (bijvoorbeeld 'boardroom dynamics') onwenselijke risico's voor de betreffende financiële instelling zijn te onderkennen. Zij maken daarbij gebruik van diverse onderzoeksmethodes. Het aldus uitgeoefende toezicht is risicogericht zonder daarbij een vast kader of ideaalbeeld van cultuur voor ogen te hebben. Dat DNB met deze benadering naar eigen bevinden succes heeft geboekt en in gevallen tot waardevolle aanbevelingen heeft kunnen komen, is voor het in deze bijdrage gekozen punt van vertrek betekenisvol aangezien ook hierin het gebruikmaken van de relatie tussen cultuur en risico wordt voorgesteld.

Afgeleid uit de vele bestaande definities en omschrijvingen, wordt organisatiecultuur in het vervolg van deze bijdrage begrepen als: de gedeelde overtuigingen, waarden, normen, en gedragingen die de algehele werkomgeving bepalen en richting geven aan het handelen en de beslissingen van individuen binnen een organisatie.

De sleutel tot het 'vormgeven' van cultuur ligt derhalve in de onderliggende normen en waarden als zijnde sturend voor gedrag. Andere artefacten en producten die de cultuur kenmerken en die ook individueel te adresseren zijn, zijn bijvoorbeeld de ondernemingsvisie en -missie, de uitgedragen kernwaarden, beslissingsmodellen en bijbehorende processen en gedelegeerde bevoegdheden, beleidsrichtlijnen en regels ('policies'), de mate van samenwerking en teamwork, en de algehele werksfeer. Zelfs de gecreëerde werkomgeving inclusief de kantoorinrichting, de kantine en de eventuele (al dan niet gratis en al dan niet gezonde) snacks kunnen als manifestatie van de cultuur beschouwd worden. Het is daarbij belangrijk te beseffen dat de waarneembare en onzichtbare elementen van cultuur elkaar wederzijds kunnen (en zullen) beïnvloeden. Zo is de werkomgeving (gesloten werkruimtes versus de open kantoorruimte) een manifestatie van de cultuur maar beïnvloedt zij omgekeerd ook hoe mensen met elkaar samenwerken.⁶

5 DNB/M. Raaijmakers (red.), *Supervision of Behaviour and Culture: Foundations, practice & future developments*, De Nederlandsche Bank 2015, <https://www.dnb.nl>.

6 Post-COVID is aan deze vergelijking het 'nieuwe werken' toe te voegen, waarover verschillende opvattingen zijn gaan leven en voorkeuren ontstaan tussen generaties, groepen werknemers en tussen bedrijfstakken – eveneens te zien als een uitvloeisel van culturele verschillen.

2.2 Effectiviteit van cultuur ('culturele effectiviteit')

In een omvangrijk praktijkgericht onderzoek hebben Graham en collega's⁷ de vraag centraal gesteld naar wat een cultuur 'effectief' maakt. Zij gaan daarbij uit van een model waarin deze waarneembare en onzichtbare elementen van cultuur in hun onderlinge samenhang en wisselwerking worden gezien. In dit model spreken zij van waarden ('values') als 'big principles', en normen ('norms') als 'day-to-day practices', die gezamenlijk richting geven aan gedragingen en beslissingsprocessen om uitvoering te geven aan de strategie en invulling van doelstellingen. Zij benoemen verder 'formal institutions' als de formele elementen van corporate governance om gedragingen en beslissingsprocessen te beheersen, zoals bijvoorbeeld organisatie-structuren, codes, regels en richtlijnen, HR-procedures en het belonings- en bonus-beleid. Zij definiëren vervolgens de effectiviteit van cultuur – culturele effectiviteit – als de mate waarin de cultuur gedragingen stimuleert die bijdragen aan succesvolle uitvoering van de strategie en het bereiken van doelstellingen. Zij stellen dat de culturele effectiviteit afhangt van de samenhang en interactie tussen de waarden, normen en de 'formal institutions':

"The values and norms characterize the structure in place that guides employees' actions when they face unforeseen contingencies. A cultural value represents an ideal state of behavior such as integrity or adaptability. Cultural norms are the day-to-day living out of the cultural values via the typical patterns of conduct. An effective culture is one that promotes the behaviors needed to successfully execute the firm's strategies and achieve its goals. The effectiveness of culture is determined by the alignment of and interactions between values, norms, and formal institutions."

De koppeling door de onderzoekers van een individuele kernwaarde – 'cultural value' – aan een bepaald soort gedrag – 'state of behavior' – is van belang voor het vervolg. Als we culturele effectiviteit begrijpen, kunnen we met behulp van de aangetoonde relatie tussen waarden en normen en gedrag een duidelijkere link leggen met het managen van risico. Voor we hier dieper op in kunnen gaan, kaderen we eerst nog het begrip risico en de betekenis van risicomanagement in.

3. Risico en risicomanagement

3.1 Risico

Ook al levert googelen op het woord 'risk' thans zo'n 8,5 miljard hits op, zoals opgemerkt in de inleiding lijkt het concept van risico in haar samenstellende delen dikwijls niet volledig begrepen. Intuïtief voelen wij vaak wel aan wat risico is en eenieder die zijn veiligheidsgordel omdoet in de auto of een valhelm draagt begrijpt de basisbeginselen van risicomanagement. Het is goed om te beseffen echter, dat wij toch niet zo goed zijn in het juist inschatten van (kansen en) risico's als gevolg van

⁷ J.R. Graham, J. Grennan, C.R. Harvey & S. Rajgopal, Corporate culture: Evidence from the field, *Journal of Financial Economics* 2022, 146(2), p. 552-593.

diverse vormen van ‘bias’ en het verkeerd veronderstellen van (scheve) kansverdelingen, zoals uitgebreid beschreven door Taleb.⁸ Zonder thans uitgebreid op alle aspecten van risico-inschattingsproblematiek in te gaan, is het voor het voorgestelde ‘risicoperspectief’ als vertrekpunt voor ‘toezicht op cultuur’ wel onvermijdelijk om eerst het begrip risico nader uit werken, en daarmee ook wat risicomanagement meer precies inhoudt. Omgaan met cultuur vanuit risicoperspectief vereist immers niet alleen een goed begrip van cultuur, maar ook van risico.

Een beter begrip van het concept ‘risico’ begint door het te zien als het onlosmakelijke gevolg van het stellen (hebben) van doelen, onder invloed van de onvermijdelijke factor onzekerheid. Doelen worden gesteld omdat zij een bepaald belang vertegenwoordigen. Omdat doelen inherent betrekking hebben op de toekomst zijn zij altijd onderhevig aan risico. De toekomst is immers nooit met absolute zekerheid vast te stellen en onverwachte gebeurtenissen kunnen zich met een bepaalde kans te allen tijde voordoen, ook al is de waarschijnlijkheid daarvan grotendeels gebonden aan de factor tijd. Pas bij het (expliciet) stellen van doelen die verder weg liggen in de tijd, of bij heel duidelijk te onderkennen en in te schatten kortetermijnrisico’s (‘bust’ of ‘kapotgaan’ bij een extra kaart in een ronde aan de blackjacktafel, mogelijkerwijs struikelen op een modderig talud vlak vóór de te wagen sprong over de sloot) stemmen wij welbewust onze beslissingen (al dan niet ‘passen’ bij 17) en handelingen (de aanlooproute grondig verkennen) hierop af. Als de afzienbare termijn van een doelstelling zich voorbij een daaraan verbonden (subjectief ervaren) tijdshorizon strekt zijn wij echter weer geneigd de langetermijnrisico’s te negeren of te bagatelliseren en het nemen van als onprettig ervaren maatregelen in het kader van het onderhavige belang uit te stellen.⁹

Of we het bewust onder ogen zien en ernaar handelen of niet: zonder een vanuit een zeker belang beoogd doel treden risico’s simpelweg niet op. Dan is ook het management of beheersing daarvan niet aan de orde. Het omdoen van de veiligheidsgordel heeft alleen zin als er sprake is van een reisdoel met als randvoorwaarde het efficiënt en veilig bereiken daarvan: niet als men geparkeerd staat en slechts in de auto gaat zitten om even rustig te kunnen telefoneren. Uit dit simpele voorbeeld valt af te leiden dat doelen zowel min of meer expliciet (ik wil van A naar B; of ik wil iemand telefonisch spreken) of impliciet (snel, comfortabel, veilig; of ongestoord) gesteld kunnen worden – al is dat vaak in onderlinge samenhang. Wel kunnen al dan niet met elkaar samenhangende doelen verschillen in belang, en kunnen deze worden gerangschikt. Het veilig bereiken van punt B kan wel eens belangrijker zijn dan dat dit zo comfortabel mogelijk geschiedt (een ‘nice-to-have’ in dit voorbeeld). De snelheid waarmee het gebeurt kan ook zwaar wegen, en dan kunnen we de kortste weg met het risico op file maar beter vermijden of een ander vervoermiddel kiezen. Risico vraagt om risicomanagement en daar is de belangenafweging een essentieel onderdeel van.

8 N.N. Taleb, *Fooled by Randomness: The hidden role of chance in life and in the markets*, New York (NY): Random House 2004, 2016.

9 Dit fenomeen is een belangrijke factor in bijvoorbeeld het volgens de wetenschappers niet snel genoeg verminderen van emissies (met alle mogelijke gevolgen van dien in de verdere toekomst) of het feit dat velen worstelen met het verbeteren van gewoonten die de eigen gezondheid op langere termijn aangaan.

Bij ondernemingen en publieke organisaties vinden we expliciet geformuleerde doelen in de vorm van de missie en strategische of tactische doelstellingen en 'targets'. Deze hebben voornamelijk waardecreatie en/of -behoud¹⁰ op het oog, op zowel de lange als kortere termijn. Impliciete doelstellingen zijn meer gericht op waardebehoud, zoals bijvoorbeeld het voldoen aan wet- en regelgeving, het handelen in overeenstemming met algemeen geldende waarden en normen, en veiligheid. Deze kunnen dan als het ware als randvoorwaarden worden beschouwd, of zijn weliswaar (deels) opgenomen in codes en voorschriften, maar niet zozeer een direct onderdeel van de ondernemingsstrategie (van A naar B gaan). Vraag een CEO wat diens prioriteiten zijn, en zelden zal de veiligheid van het personeel als eerste worden genoemd. Op de vraag echter of de CEO de bedrijfsveiligheid van cruciaal belang vindt zal in de meeste gevallen het volmondige antwoord bevestigend luiden. Dus ook impliciete doelen kunnen zwaar meetellen. Voor de risico's die zich daartegenover kunnen voordoen wordt in dit verband ook wel gesproken van 'rewarded' versus 'unrewarded' risks.

3.2 *Dimensies van risico: impact, vulnerability en probability*

In zowel expliciete als impliciete vorm veroorzaakt een doel met een daaraan te hechten belang dus risico. Het risico bestaat er in principe uit dat het betreffende doel mogelijkerwijs niet (geheel) zal worden gehaald, dan wel niet constant/consistent (bijvoorbeeld het voorgenomen percentage 'up-time' van een onlineservice). Dit vanwege onzekere gebeurtenissen en onvoorziene omstandigheden. Het onderhavige belang wordt daarmee geschaad.¹¹ De mate van afwijking van het doel, de schade aan het belang, wordt wel aangeduid met 'impact', en dit begrip zal ook ik in de rest van deze bijdrage hanteren om het gevolg c.q. de gevolgen aan te duiden van een risico dat materialiseert. Voor het goede begrip: toekomstige, onzekere gebeurtenissen kunnen impact hebben op meerdere doelen en belangen (tegelijk) en tevens kan vervolgschade zich in veel gevallen voordoen. Echter, zoals hierboven opgemerkt: niet elk doel – zij het expliciet of impliciet – vertegenwoordigt een evenredig belang. Als we 'impact' beschouwen als de eerste dimensie van risico (schade aan het belang), dan is het belang van het doel – oftewel de prioriteit – de eerstvolgende, tweede dimensie. Ons begrip van impact dient dan ook te allen tijde gekoppeld te worden aan het belang daarvan. Het (grotendeels) missen van sommige gestelde doelen kan tot een schouderophalen leiden, terwijl het missen van andere doelen desastreuze gevolgen kan hebben voor de duurzame langetermijnwaardecreatie (of zelfs het voortbestaan van de onderneming) en de belangen van al haar stakeholders. Naarmate het belang van het doel groter is, neemt de kwetsbaarheid

10 Hieronder kunnen ook worden begrepen het minimaliseren van ingecalculerd waardeverlies op basis van een strategische keuze zoals bijvoorbeeld uitfasering van een business of een product, of een tactische reactie op een negatieve ontwikkeling (een materialiserend risico), bijvoorbeeld bij het plotseling uitvallen van leveranties: snel een betrouwbare nieuwe leverancier vinden.

11 Voor de volledigheid heeft meer recent het idee dat risico naast een 'downside' ook een 'upside' kant zou hebben aan populariteit gewonnen. Ik ben geen voorstander van deze tegennatuurlijke – zo niet onjuiste – interpretatie van risico. Wel valt te onderkennen dat de factor onzekerheid evenzeer onverwachte mogelijkheden en doel bevorderende kansen kan aanreiken. Ik ga op het te maken onderscheid tussen 'risk' en 'opportunity' hier verder niet in.

voor een afwijking van dat belang – belangenschade – toe. Vandaar dat dit ook wel wordt gevangen in de term ‘vulnerability’. Het onderkennen van vulnerability als tweede dimensie van risico naast impact is van essentieel belang voor het begrijpen en evalueren van risico. Prioriteiten zijn veranderlijk in de tijd én naargelang de omstandigheden (en vulnerability dus ook). Voor een naderende regenbui in het open veld biedt het tijdig schuilen onder die enkele grote boom wellicht de nodige bescherming, maar het belang om droog te blijven wordt ondergeschikt aan het belang om te overleven als de naderende regen gepaard gaat met onweer en bliksem: dan is het schuilen onder dezelfde boom een slecht idee.

Naast impact wordt in de praktijk veel aandacht gegeven aan de analyse van ‘probability’ – ook wel ‘likelihood’ – van mogelijke gebeurtenissen (‘events’) om risico’s te taxeren en hierover te rapporteren. Risico wordt dan ook nog wel eens uitgedrukt als ‘impact x probability’. De traditionele ‘heatmap’ (met bijbehorende risicomatrix) is daar een goed voorbeeld van. Het hanteren van probability kent echter een aantal mogelijke struikelblokken. Probability is bijvoorbeeld gevoelig voor inschattings- en beoordelingsfouten (zie ook Taleb, hierboven aangehaald), is bovendien variabel in de tijd en in veel gevallen beïnvloedbaar, bijvoorbeeld door interne controlemaatregelen (denk bijvoorbeeld aan cyber-risicobeheersing). Dit uit zich soms ook in spraakverwarring tussen ‘inherent’ en ‘rest-’ of ‘netto-*risico*’ (hetgeen overblijft na de genomen beheersingsmaatregelen, uitgaande van de effectiviteit daarvan). Door een grote focus op probability kunnen de zogenaamde ‘black swan events’¹² (bijvoorbeeld ‘9/11’) onderbelicht blijven en kunnen daartegenover de te onderkennen ontwikkelingen die bij ongewijzigd beleid een bijna zekere afwijking van een doel zullen veroorzaken (een zeer hoge probability hebben, zoals bepaalde te verwachten veranderingen in wet- en regelgeving) vragen om ingrijpen dat – terzijde – nog nauwelijks voor risicomanagement kan doorgaan: eerder een correctief handelen of zelfs crisismanagement.

Samengevat: de statistische kans (probability) dat een grote meteoriet inslaat op een productiesite die de continuïteit van de productie zou bedreigen (impact), en daarmee het voortbestaan van de gehele onderneming (vulnerability) – nog afgezien van de veiligheid van het aanwezige personeel (ook: impact) – is zodanig verwaarloosbaar dat het treffen van beschermende maatregelen realistisch en economisch gezien zinloos is en bovendien praktisch onhaalbaar. Dan rest acceptatie van dit risico, maar kan er wel beoordeeld worden of impact-mitigerende maatregelen (zoals spreiding van productie en het afsluiten van verzekeringen) mogelijk en verstandig zijn. Deze maatregelen zien immers niet alleen toe op de precieze denkbeeldige gebeurtenis zelf (de meteoriet) maar ook op andere scenario’s die de continuïteit van productie zouden kunnen bedreigen. Uiteraard passen daarbij wel probability-inschattingen, zoals hier te lande overstromingsgevaar versus het gevaar van een vulkaanuitbarsting. Meer toegespitst op risico’s bezien vanuit de cultuur, zijn bijvoorbeeld met

12 Overigens is het ook aan Taleb toe te schrijven dat het begrip ‘black swan events’ als zodanig brede erkenning heeft gevonden. N.N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, New York (NY): Random House 2007, 2010.

name multinationals blootgesteld aan een van regio tot regio variërend gevaar van vigerende omkopings- en corruptiepraktijken. De internationaal strenger wordende wet- en regelgeving (naar voorbeeld van de US FCPA met haar extraterritoriale werking) met zware boetes en mogelijke criminele vervolging van bestuurders werkt vulnerability verzwarend. Ook het Volkswagen 'Dieselgate'-schandaal illustreert opnieuw hoe een op het eerste oog laag in te schatten probability van een dergelijke vorm van frauduleus gedrag samenvloeit met een hoge vulnerability ten aanzien van de impact. Hiertegenover staat dan logischerwijs een lage risicotolerantie binnen het gewenste risicoprofiel en beheersingsmaatregelen die hierop zijn afgestemd (zie ook de subparagraaf 'risicomanagement' hieronder). Een focus op vulnerability met een pas in tweede instantie in aanmerking te nemen probability (en gehanteerd met de daarbij benodigde omzichtigheid) kan in de praktijk tot betere inzichten en beslissingen leiden. Hierop valt af te dingen dat een kwantitatieve risico-inschatting in sommige gevallen goed mogelijk, nuttig of zelfs noodzakelijk is (bijvoorbeeld in financiële instellingen en bij inschattingen rond financiële risico's zoals krediet- en verzekeringsrisico's of bij investeringsbeslissingen en waarderingen). Ik zal in het kader van deze bijdrage hier verder niet dieper op ingaan, maar in het kijken naar cultuur gerelateerde risico's wel een benadering voorstaan die op grond van bovenstaande primair uitgaat van de prioriteiten van de belangen en de potentiële schade daaraan, waarbij probability als de mogelijk derde in aanmerking te nemen dimensie van risico wordt beschouwd, door middel van het beoordelen van risicofactoren. Dit laatste zal ik verderop nader toelichten.

De managementtheorie heeft meerdere risicomodellen en -frameworks voortgebracht, die hun toepassing vinden in de praktijk van risicomanagement. Categorisering van risico's in deze modellen is niet altijd even nuttig en levert soms de vraag op in welke categorie een risico valt. Zo kan een compliance risico (bijvoorbeeld indien kritisch voor een vergunning) tevens een strategisch risico betekenen. Een data security breach kan afhankelijk van het geval zowel als een intern als extern risico beschouwd worden, maar ook vanuit compliance opzicht (waarbij de geleden reputatieschade of de mogelijke boete zelf als een mogelijk strategisch issue valt te bezien). In het model van Kaplan en Mikes¹³, worden risico's als volgt onderscheiden: strategisch, extern en intern. Dit lijkt niet bijster origineel, maar de praktische waarde van hun bijdrage is dat zij de risico's feitelijk onderscheiden naar en koppelen aan de wijze waarop deze kunnen worden benaderd en (effectief) gemanaged. Zij schetsen dan ook voor elk van deze soorten risico een eigen benadering en een set maatregelen om de risico's te identificeren, te managen en te optimaliseren. Het strategische risico (te zien als 'rewarded') ontstaat vanuit de strategische keuzes en beslissingen die liggen besloten in het ondernemen en het stellen van de ondernemingsdoelstellingen: hier is het kennen, begrijpen, en bewust accepteren van te nemen risico's die horen bij de strategische beslissingen de aangewezen weg. De mate van intelligentie toegepast op die beslissingen, spreiding, vermijden en monitoring brengen c.q. houden risico's op een gewenst niveau. Interne risico's (ook

13 A. Mikes & R.S. Kaplan, 'Managing risks: A new framework', *Harvard Business Review* 2012, 90(6), p. 48-60.

wel ‘rewarded’, zoals bij belangrijke projecten, maar veelal ‘unrewarded’, zoals in het geval van een fout in de belastingaangifte) zijn de risico’s in de uitvoering van de ondernemingsstrategie en de dagelijkse processen. Deze soorten risico’s zijn te beheersen zijn door diverse interne controlemaatregelen,¹⁴ oftewel het interne controlesysteem. Externe risico’s (‘unrewarded’) zijn in het algemeen niet te beïnvloeden en vragen primair om impactbeperkende maatregelen, zoals in het voorbeeld van een rampenscenario hierboven gegeven.

Voor het verschijnsel cultuur, staan de gedragingen die daar een uitvloeisel van vormen vooral in verhouding tot hoe beslissingen worden genomen op het strategische en tactische vlak die mogelijk impact hebben op het (geheel) bereiken van doelen of doelstellingen. Zoals in paragraaf 2.1 besproken, met als sleutel tot het ‘vormgeven’ van cultuur de onderliggende normen en waarden die gedrag sturen, maakt dit dat gedrag gerelateerde risico’s in het model van Kaplan en Mikes als ‘intern’ te bestempelen zijn, oftewel ‘beheersbaar’. Hier kom ik onderstaand nog op terug in de subparagraaf risicomangement.

Het uiteindelijke ondernemingsdoel wordt in de Code volgens Principe 2.5 algemeen aangeduid met duurzame langetermijn¹⁵ waardecreatie. Met duurzaam wordt dus een bredere opvatting van waarde gehanteerd – in de zin van ‘profit, planet & people’ – hetgeen zijn weerklank vindt in de huidige toenemende duurzaamheidsrapportagevereisten, bijvoorbeeld vanuit de CSRD. Dit heeft als gevolg dat duurzaamheid en regelgeving daaromheen alsmede rapportagedruk – mede op basis van de vereiste dubbele materialiteitsanalyse – meerdere dimensies aan het risicoprofiel van de onderneming heeft toegevoegd (zowel in rewarded als unrewarded opzicht) en kijkend naar culturele effectiviteit is dit relevant. Indien bijvoorbeeld door een bepaalde onderneming het welzijn van werknemers als een vooropstaand doel wordt beschouwd, dienen naast traditionele financiële aspecten de risico’s rond werknemerswelzijn de volle aandacht te krijgen en te worden gemanaged, en hierover te worden gerapporteerd. Het is daarom noodzakelijk om te begrijpen hoe het algemeen geformuleerde doel in de Code in de praktijk voor een organisatie concreet en in meer detail wordt ingevuld vanuit de visie en de missie – de ‘purpose’ – en strategie (en de dubbele materialiteitsanalyse), aangezien hieruit de prioriteiten zijn af te leiden. Deze geven richting aan de risicoanalyse, in het kader van deze bijdrage specifiek in relatie tot de cultuur.

14 Over hoe risicomangement en met name het interne controlesysteem zich in de praktijk kan laten vormgeven is het nodige geschreven en zijn diverse ontwikkelde frameworks, standaarden en practice guidelines te raadplegen. Bijvoorbeeld COSO en ISO en specifiek met betrekking tot IT en cyber security onder meer COBIT, ISO, NIST en ITIL. Het voert te ver om hier nu uitgebreid op in te gaan.

15 De toevoeging van de langetermijnhorizon ten aanzien van waardecreatie zou moeten voorkomen dat kortetermijnbeleid op enig van deze waarde-aspecten de overhand zou krijgen – ter verdere versterking van de gerichtheid op duurzaamheid.

3.3 *Risicomanagement: het optimaliseren van risico's*

Risico's in het kader van ondernemerschap en goede corporate governance zijn er niet om geëlimineerd te worden (hetgeen het elimineren van ondernemingsdoelen en het negeren van belangen van stakeholders zou betekenen), zelfs niet per se geminimaliseerd: dit gaat immers gepaard met kosten van risicobeheersingsmaatregelen ofwel het veronachtzamen van groeikansen. Soms is in de trade-off méér risico gewenst om waarde te creëren, en soms minder. Daarom gaat het er bij risicomanagement in de eerste plaats om de organisatie te bewegen binnen (of zelfs 'op') de grenzen van het optimaal geachte risicoprofiel. In de praktijk gehanteerde begrippen in dit kader zijn ook wel 'risk appetite' of 'risk tolerance'. Hoewel deze begrippen van elkaar verschillen, worden deze dikwijls door elkaar heen gebruikt. Gemakshalve spreek ik verder van het 'gewenste risicoprofiel'. Het is belangrijk om op te merken dat deze door meerdere factoren wordt beïnvloed: zowel extern (bijvoorbeeld bij financiële instellingen vanuit de regelgeving) en vanuit bedrijfs-economisch opzicht (de financiële capaciteit om bepaalde soorten risico's te dragen), maar zeker ook door bestuurders en de verschaffers van kapitaal, welke deels subjectief – en dus ook cultureel – bepaald kunnen zijn.

Zoals hiervoor besproken bieden Kaplan en Mikes de nodige handvatten om risicobeheersing gericht toe te passen. Kijkend naar risico's vanuit de organisatiecultuur gaat het dan dus om beheersbare, oftewel als 'intern' aan te merken risico's. Natuurlijk bestaan er mogelijkserwijs ook 'externe' risico's die versterkt kunnen worden vanuit (macro)culturele invloeden (bijvoorbeeld het risico op sociale en politieke onrust), welke echter niet of nauwelijks beheersbaar zijn door interne controlemaatregelen. De 'strategische' risico's volgen, zoals hierboven gesteld, vanuit de keuzes en strategische beslissingen vanuit de purpose en de doelstellingen. De gedragingen die aan deze beslissingsprocessen ten grondslag liggen bepalen voor een groot deel de culturele effectiviteit, en de risicobeheersing zou zich dus moeten richten op de processen, de waarden, en daarmee de gedragingen op het niveau waarop deze beslissingen worden genomen. Een interessante ontwikkeling in dit verband is de toenemende aandacht voor de 'soft controls'. Soft controls zijn de niet-tastbare gedragsbeïnvloedende factoren in een organisatie die van belang zijn voor het realiseren van de purpose van de organisatie (Van Bakkum)¹⁶. Zo bezien dragen effectieve soft controls – lees: 'vormgeven van de cultuur' – dus bij aan het interne controlesysteem, en aan risicomanagement. Omgekeerd kunnen risico's in de cultuur een bedreiging vormen voor het behalen van succes in het realiseren van de purpose, en met dit inzicht zal ik onderstaand een risicogedreven proces van toezicht nader uitwerken.

¹⁶ E. van Bakkum, 'Een effectieve purpose wortelt in cultuur en gedrag', in: Lückerath-Rovers e.a. (red.), *Jaarboek Corporate Governance 2020-2021*, Deventer: Wolters Kluwer 2020, p. 119-136.

4. Toezicht op cultuur: een proces in vijf stappen

Aan het eind van de eerste paragraaf heb ik de vijf stappen van het voorgestelde proces geïntroduceerd. Deze zijn in Diagram 1 nogmaals weergegeven, en ik licht deze stappen onder verwijzing naar de in de aanloop gemaakte verduidelijking van cultuur en risico (in hun samenhang) hieronder verder toe.

Diagram 1: Proces voor risicogedreven toezicht op cultuur



4.1 Vaststellen prioriteiten

Zoals in paragraaf 3.1 hierboven omschreven is het voor het inschatten van risico essentieel om te begrijpen wat de belangrijkste doelen zijn: zowel in expliciete als impliciete zin. Pas vanuit een grondig en gedeeld begrip van ‘what must go right’ kan een beeld over impact van en vulnerability voor de belangrijkste risico’s – ‘what might go wrong’ – worden opgebouwd. Helderheid over de prioriteiten is de resultante van regelmatig en vruchtbaar overleg tussen de RvC en het bestuur, en deze prioriteiten dienen volgens de Code te zijn herleiden tot duurzame langetermijn-waardecreatie. Afhankelijk van veranderende markt- en omgevingsfactoren en strategische beslissingen – gestuurd door de purpose – kunnen prioriteiten in de loop der tijd wel verschuiven, zoals in het voorbeeld gegeven van regen in combinatie met naderend onweer in de omschrijving van risico.

4.2 Aansluiten kernwaarden

Zijn de prioriteiten die voor het moment gelden helder vastgesteld, dan kan worden bepaald welke kernwaarden in de cultuur hierop qua relevantie het nauwst aansluiten. Hoe deze ‘mapping’ er op enig moment uitziet voor de betreffende organisatie hangt dus af van de prioriteiten en hoe de kernwaarden gedefinieerd zijn en dit maakt een groot aantal variaties mogelijk.

Het eerder aangehaalde praktijkonderzoek door Graham en collega’s gaat uit van zeven categorieën van ‘cultural values’, die door hen zijn afgeleid uit de literatuur en gebaseerd op diverse onderzoeken. Deze cultural values zal ik in het vervolg verder als ‘kernwaarden’ aanduiden. Met enige vrijheden in de interpretatie, kunnen deze als volgt worden onderscheiden, waarbij ik de vertaling naar het Nederlands gemakshalve achterwege laat:

- Adaptability: open to change, willing to experiment, fast-moving, quick to take advantage of opportunities, taking initiative, being innovative.
- Collaboration: team-oriented, supportive, not aggressive, low levels of conflict, open and honest communication.

- Community: respectful of diversity, community, and the environment; inclusive, caring, and open to the broad group of stakeholders.
- Customer-orientation: listening to customers, being brand-driven, taking pride in service and having trustful (long-term) relations.
- Detail-orientation: paying attention to detail, being precise, emphasizing quality and safety, being analytical, being diligent, and risk-aware.
- Integrity: high ethical standards towards business conduct, being honest, transparent.
- Results-orientation: high expectations for (sustainable) performance, focus on achievement of both short-and long-term goals, competitive, demanding.

Indien we de generieke doelstelling van de Code nemen en, in tweeën gesplitst, toepassen om als illustratief voorbeeld van ‘mapping’ uit te werken, dan zou uitgaande van de individuele relevantie van de kernwaarden voor de centrale doelstellingen de aansluiting er, zoals in Tabel 1 weergegeven, uit kunnen zien.

Tabel 1: Illustratief voorbeeld van aansluiten relevantie kernwaarden met prioriteiten

Kernwaarde	Langetermijngerichtheid	Duurzame waardecreatie
Adaptability	Hoog	Gemiddeld
Collaboration	Laag-Gemiddeld	Gemiddeld
Community	Hoog	Hoog
Customer-orientation	Hoog	Hoog
Detail-orientation	Gemiddeld	Gemiddeld-Hoog
Integrity	Hoog	Hoog
Results-orientation	Hoog	Hoog

Het doel van een dergelijke mapping is om in gezamenlijk overleg te bepalen welke kernwaarden het meest bijdragen aan de culturele effectiviteit. Hier zal vervolgens de focus voor het taxeren van de risico's op moeten komen te liggen, na het evalueren van de te onderkennen risicofactoren. Zoals hierboven aangegeven, zal deze mapping in de praktijk een groot aantal variaties kennen.

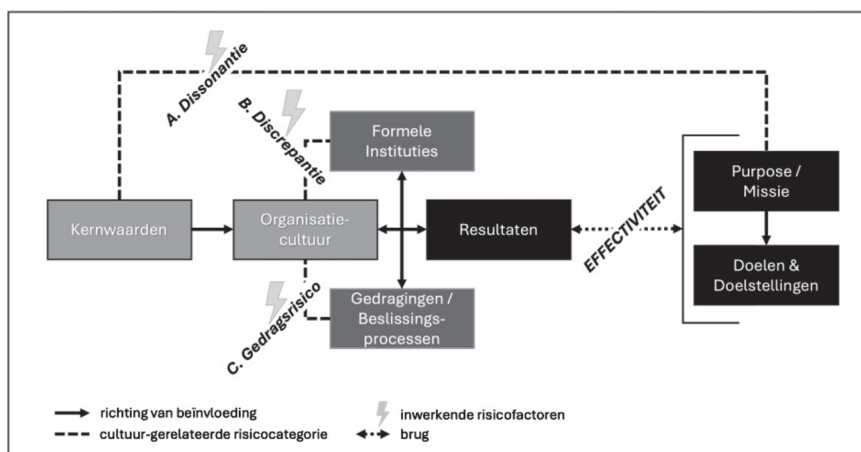
4.3 Evalueren risicofactoren

4.3.1 Model voor culturele effectiviteit

In Diagram 2 worden, naar het model van Graham en collega's, de relaties tussen de organisatiecultuur, formele instituties en gedragingen en beslissingsprocessen (de laatste twee zijnde ‘artefacten’) getoond. Zoals geïllustreerd beïnvloeden deze elkaar onderling en wederzijds. De artefacten zijn een gevolg van de organisatiecultuur en vice versa, terwijl de in de vorige subparagraaf besproken kernwaarden

bepalend zijn voor de cultuur. Wanneer de resultaten dicht bij de purpose, het doel en de doelstellingen liggen (dat wil zeggen: er is weinig afwijking), is er sprake van culturele effectiviteit.

Diagram 2: Model van culturele effectiviteit en gerelateerde risicocategorieën



Uit de geschetste relaties in Diagram 2 zijn drie afzonderlijk te onderscheiden hoofdcategorieën van risico's voor culturele effectiviteit te distilleren. Deze zal ik verder aanduiden als: dissonantie, discrepantie, en gedragsrisico, oftewel: risico van ongewenste gedragingen.

A. Dissonantie

Als de purpose/missie niet goed is verankerd in culturele waarden en normen (kernwaarden), resulteert er dissonantie die de verwezenlijking van doelen negatief kan beïnvloeden. Bijvoorbeeld, een meetbaar laag niveau van de kernwaarde 'customer-orientation' zal het bereiken van een doel dat de focus legt op klantgerichtheid niet ondersteunen. Omgekeerd moet de organisatiecultuur ontvankelijk zijn voor de missie en de gekozen doelen en doelstellingen om gedrag en besluitvorming in de richting van succes te sturen.

B. Discrepantie

Om de bedrijfscultuur effectief te laten werken, moeten de formele instituties, inclusief maar niet beperkt tot het systeem van interne controle, overeenkomen. Bijvoorbeeld, een gewenst hoog niveau van de kernwaarde 'collaboration' kan worden belemmerd in een gesloten kantooromgeving (en, volgens sommigen, in bedrijven die een hoge mate van thuiswerken toestaan). Een (zeer) strak intern controlesysteem kan als verstikkend worden ervaren in een cultuur met een lage 'detail-orientation' in combinatie met hoge 'adaptability'. Omgekeerd kan in sterk gereguleerde industrieën (bijvoorbeeld financiële dienstverlening) een zeer strak en formalistisch intern controlesysteem juist nodig zijn om te voldoen aan de regelgeving, en de

bedrijfscultuur zou ontvankelijk moeten zijn om dit te ondersteunen (hoge mate van 'detail-orientation'). Mogelijke discrepanties in die zin doen zich regelmatig voor in een post-overnamescenario, bijvoorbeeld wanneer het overnemende bedrijf procesmatige eisen en systemen oplegt aan de overgenomen partij wiens cultuur daar niet ontvankelijk voor is. Bovendien kan de afwezigheid (of ineffectiviteit) van een formele institutie zoals een klokkenluiderfaciliteit of een vertrouwenspersoon voor het melden van (seksueel) wangedrag of pesten de niveaus van integriteit en samenwerking beïnvloeden en een sociaal werkklimaat creëren dat onvoldoende veilig is (Spoor & Riethof¹⁷). De nagestreefde culturele waarden moeten ook voldoende transparant worden gemaakt en worden begrepen via formele instituties, bijvoorbeeld door middel van communicatieprogramma's en training; zo niet, dan kunnen discrepanties ontstaan.

C. Gedragsrisico

Ten aanzien van het (gewenste) gedrag en beslissingsprocessen kunnen verschillende risico's optreden, met een van mild tot ernstig variërende impact. Deze risico's betreffen bewuste (in dat geval spreken we al snel van ernstig) dan wel onopzettelijke afwijking van de kernwaarden van de organisatie. Mildere afwijkingen kunnen worden veroorzaakt door onvoldoende absorptie en kennis van de waarden (wellicht te wijten aan discrepantieproblemen, zoals gebrek aan communicatie daaromtrent) of door een oprechte beoordelingsfout (bijvoorbeeld in een internationale omgeving door spanningen tussen lokale macroculturele waarden en normen en de kernwaarden die de onderneming voorstaat, of binnen divers samengestelde teams¹⁸). Bewuste vormen van wangedrag – gefaciliteerd door zwakheden in het interne controlesysteem – omvatten (als voor de hand liggend voorbeeld) fraude, maar ook heimelijke risiconeming buiten de vastgestelde parameters of bevoegdheidsniveaus. Bijvoorbeeld wanneer er sprake is van hoge druk om bepaalde resultaten te bereiken en het beloningssysteem daar eenzijdige focus op legt. Tot slot is falend leiderschap dat er niet in slaagt om het goede voorbeeld te geven en de culturele waarden na te leven, een belangrijke oorzaak van ongewenste gedragingen op de lagere niveaus van de organisatie. Schein, bovenstaand aangehaald, wijst erop dat leiderschap en cultuur twee kanten van dezelfde medaille zijn. Soms ernstige reputatieschade – en daarmee waarde-erosie – kan ontstaan als een onderneming (als een projectie van het gedrag van haar leiders) in de ogen van het publiek niet voldoet aan de geformuleerde purpose en doelstellingen – en daarmee feitelijk culturele ineffectiviteit demonstreert.

4.3.2 Risicofactoren

Voor de risicoanalyse zijn in aanmerking te nemen risicofactoren medebepalend. In de bovenstaande omschrijving van de risicocategorieën zijn al enkele voorbeelden

17 S. Spoor & H. Riethof, 'Het lastige gesprek blijven voeren: Hoe te signaleren en acteren als toezichthouder ten behoeve van sociale veiligheid in organisaties', in: Lückérath-Rovers e.a. (red.), *Jaarboek Corporate Governance 2023-2024*, Deventer: Wolters Kluwer 2023, p. 111-124.

18 Trompenaars en Hampden-Turner, hierboven aangehaald, wijzen in dit opzicht op het mogelijk anderszins bestaan van, te overbruggen, dilemma's.

gegeven van risicofactoren. Risicofactoren dragen bij aan de ‘probability’ dat een risico die de culturele effectiviteit aantast materialiseert, en daarmee de relevantie van dat risico. In de analyse gaat het er niet om deze ‘probability’ met precisie vast te stellen (zoals hierboven besproken), maar vooral of er een factor van betekenis in het spel is ten aanzien van de desbetreffende risicocategorie.

Het voert te ver om te trachten een uitputtende lijst van potentiële risicofactoren op te stellen, welke situatie-afhankelijk is, maar het overzicht in Tabel 2 kan als leidraad dienen voor een dergelijke analyse. Sommige factoren dragen mogelijk- wijs bij aan meerdere categorieën.

Tabel 2: Potentiële risicofactoren ten aanzien van de risicocategorieën van culturele effectiviteit

A. Dissonantie	- Onvoldoende deelname van medewerkers bij het bepalen van purpose, missie en doelstellingen - Onvoldoende deelname van medewerkers bij het formuleren van culturele waarden - Overambitieuze doelstellingen/strategische doelen - Onduidelijke doelstellingen/strategische doelen - Hoog personeelsverloop en/of belangrijke veranderingen in leiderschap - Blootstelling aan internationale, crossculturele invloeden - Fusies en overnames - Het bestaan van een noodzaak voor culturele verandering
B. Discrepancie	- Complexiteit van de organisatie en/of een sterk internationale setting - Zwakheden in het systeem van interne controle (bijv. rapporten van interne/externe auditors en/of rapporten van ‘de tweede lijn’) - Lage aandacht voor cultuur door de raad van bestuur - Lage waardering voor diversiteit in rekrutering - Afwezigheid van inclusiviteit bevorderend programma - Regelmatig voorkomende fraude (zie ook bij gedragsrisico) - Zorgwekkende resultaten van medewerkerenquêtes en/of lage betrokkenheidsscores - Signalering dat de klokkenluidersfaciliteit ineffectief is (bijvoorbeeld te weinig meldingen in vergelijking met industriële gemiddelden) - Zwakke trainingsprogramma’s voor medewerkers ten aanzien van culturele waarden

	- Weinig communicatie over waarden; laag niveau van waardenherkenning - Onwenselijke dynamiek in de bestuurskamer - Gebrek aan openheid van het uitvoerend management over problemen en uitdagingen (de ‘zonzijde’ boodschap overheerst) - Verstoorde toegang tot de managementlagen en/of weinig gelegenheid geboden aan leden van de raad van commissarissen om ‘sfeer te proeven’ in verschillende delen/lagen van de organisatie
C. Gedragsrisico	- Aanwezigheid in en/of afhankelijkheid van regio’s met hoge corruptie-index scores - Rapporten die regelmatig voorkomende fraude aangeven en/of lage betrokkenheidsscores (zie ook bij discrepantie) - Meldingen van klachten, pesten, wangedrag en/of niet-naleving van regels - Dominante leiderschapsstijl van bestuurders of senior managers of anderszins ongewenst voorbeeldgedrag - Beloningssystemen die buitensporige druk kunnen veroorzaken om resultaten te leveren en/of onevenredige risiconeming bevorderen - Lage niveaus van diversiteit binnen de organisatie of in bepaalde lagen (bijv. mannelijke dominantie) - Directe observaties door leden van de RvC die op culturele tekortkomingen kunnen wijzen

4.4 Taxeren risico’s

Voor het taxeren van de risico’s (als volgende stap) is het gedeelde begrip over de prioriteiten, de daarbij aansluitende kernwaarden en de daar uitvloeiende ‘vulnerabiliteiten’ richtinggevend. Dit is de resultante van de eerste twee stappen. De overwegingen ten aanzien van de risicofactoren uit de vorige stap leiden tot het begin van een antwoord op de vraag ‘hoe groot zijn de risico’s’, waaruit voor de RvC een conclusie en een richting van handelen – actie – kan worden bepaald.

In de praktijk zal daarbij een belangrijke andere vraag moeten worden beantwoord: welke informatie en welke zekerheden over de betrouwbaarheid van die informatie heeft de RvC tot haar beschikking, en is dit bevredigend?

Het antwoord op die vraag moet komen uit een evaluatie van de geleverde ‘combined assurance’. In het concept van combined assurance worden verschillende assuranceproviders, zowel intern als extern, met variërende gradaties van onafhankelijkheid en betrouwbaarheid, in combinatie beschouwd om uitgebreide en gecoördineerde zekerheid te bieden over de effectiviteit van de risicomanagement- en

interne controleprocessen binnen de organisatie. De assuranceproviders kunnen worden vergeleken met de bekende spelers in het algemeen toegepaste ‘Three Lines Model’ van het Institute of Internal Auditors.¹⁹ Elk van de spelers in dit model kan rapporten en informatie verstrekken aan de RvC die bouwstenen voor assurance kunnen vormen. Hoe onafhankelijker en professioneler de assurancebron, des te meer zekerheid eruit kan worden afgeleid voor het onderbouwen van een conclusie over de mate van culturele effectiviteit.

Bij toepassing van combined assurance op culturele risico’s kan de RvC, met het oog op de vastgestelde belangrijkste vulnerabilities en rekening houdend met risicofactoren, schriftelijke en mondelinge rapporten gebruiken over activiteiten, en observaties en conclusies daarover, van de hoofdrolspelers:

- Bestuur (en volgende managementlaag) – eerstelijns functies: specifiek over het managen van culturele risico’s en meetresultaten van medewerkers-onderzoeken en dergelijke.
- Tweedelijns functies (zoals compliance, duurzaamheid, risico & interne controle): diverse rapportages.
- Derdelijns functies (internal audit): rapporten over de auditresultaten, waarbij de vraag gesteld kan – zou moeten – worden of het auditplan de audit van soft controls en culturele elementen naar de mening van de RvC voldoende adresseert.
- Externe assuranceproviders (soms ook wel als vierdelijns functie beschouwd) en wat zij mogelijk zeggen over risicofactoren.

Bij het combineren van assurancebronnen is het vertrouwen op management-representatie in principe even acceptabel als het vertrouwen op rapporten over activiteiten en observaties van functies in de tweede lijn, een onafhankelijke interne auditfunctie en externe assuranceproviders (externe auditors, maar ook bijvoorbeeld juridische of andere gespecialiseerde adviseurs). Echter, afhankelijk van de, door middel van de gemaakte aansluiting (‘mapping’), vastgestelde vulnerability voor tekortkomingen in de kernwaarden, nemen de eisen voor de kwaliteit en onafhankelijkheid van informatie toe, evenals de behoefte om assurance te combineren uit verschillende bronnen. De eigen observaties van de RvC, mits met de nodige zorgvuldigheid en bewustzijn van mogelijke vooringenomenheid gebruikt, kunnen deels ook assurance bieden en bijdragen.

4.5 Concluderen en handelen

Na het overwegen van de risico’s en het evalueren van combined assurance, concludeert de RvC of de cultuur van de organisatie als effectief kan worden beschouwd, of verbetering behoeft. Of de RvC bepaalt dat er voldoende basis is voor haar conclusie, hangt af van de risk tolerance, die, zoals besproken, mede is

¹⁹ Institute of Internal Auditors, *Three Lines Model: An update of the three lines of defense*, 2020, <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>.

gebaseerd op een overweging van wat er op het spel staat. De RvC wordt geacht haar verantwoordelijkheden zorgvuldig te vervullen, en daarom is de vraag: ‘hebben we genoeg gedaan?’ of ‘denken we genoeg te weten?’ valide en nodig om tot een conclusie te komen.

Indien de RvC die vraag niet naar tevredenheid kan beantwoorden, of als er een onacceptabel risico wordt geïdentificeerd ten opzichte van het gewenste risico-profiel, moet zij een adequaat corrigerend actieplan van het bestuur vragen en/of een hoger niveau van assurance van andere providers nastreven. De uitvoering van elk actieplan dient dan te worden gemonitord, en eventueel onderworpen aan (onafhankelijke) assurance.

De RvC vormt zich ook een mening over welke aspecten ten aanzien van de organisatiecultuur moeten worden opgenomen in de externe rapportage van het bestuur, zoals voorgeschreven door de Code, en bespreekt haar verwachtingen met het bestuur. Uiteindelijk zal de RvC het rapport van het bestuur beoordelen. Ten slotte dient de RvC te overwegen of er punten uit het bovenstaande naar voren zijn gekomen die in haar eigen rapport zouden moeten worden opgenomen.

5. Slotopmerking

Dit hoofdstuk is geschreven vanuit het besef: ‘Not everything that counts can be counted, and not everything that can be counted counts’. Grip krijgen op cultuur als niet meetbare grootheid kan enorm lastig zijn, en vanuit het perspectief van toezicht op de effectiviteit daarvan levert dit een zware taak op voor de RvC, waarvan het belang echter evident is: cultuur weegt nu eenmaal (zeer) zwaar. Risico, en het inschatten en managen daarvan, is evenzeer een grote uitdaging, maar bovenstaande wenken om cultuur en risico in samenhang te bezien bieden een mogelijke, hanteerbare, benaderingswijze voor de taakinvulling. Daarbij is de verwachting dat de RvC, naast bestaande en hopelijk toenemende aandacht voor cultuur, het risico-aspect reeds centraal heeft staan.